National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 30 Sep 2022 Vol. 09 No. 18

Table of Content

Vendor	Product	Page Number
next-auth	nextauth	599
Nextcloud	nextcloud	601
	nextcloud_enterprise_server	601
	nextcloud_server	603
	talk	605
nheko_project	nheko	606
nhn	toast_ui_grid	607
NI	configuration_manager	607
nic	knot_resolver	608
Ninjaforms	ninja_forms	608
Nlnetlabs	unbound	609
Nokia	1350_optical_management_system	611
notepad-plus-plus	notepad\+\+	612
notice_board_project	notice_board	613
nuprocess_project	nuprocess	613
nuxtjs	netlify-ipx	614
oauth_client_single_sign_on_project	oauth_client_single_sign_on	616
octoprint	octoprint	616
octopus	octopus_server	617
online_banking_system_project	online_banking_system	618
online_leave_management_system_project	online_leave_management_system	621
online_market_place_site_project	online_market_place_site	622
online_pet_shop_web_application_project	online_pet_shop_web_application	623
online_tours_and_travels_management_system_project	online_tours_and_travels_management_system	624
online_tours_\&_travels_management_system	online_tours_\&_travels_management_system	625
online_tours_\&_travels_management_system_project	online_tours_\&_travels_management_system	626
open5gs	open5gs	627

Vendor	Product	Page Number
Qualcomm	ipq8078a	1120
	ipq8173	1120
	ipq8174	1120
	mdm9150	1121
	mdm9206	1123
	mdm9250	1125
	mdm9607	1128
	mdm9626	1132
	mdm9628	1136
	mdm9640	1140
	mdm9650	1142
	msm8909w	1147
	msm8917	1150
	msm8920	1154
	msm8937	1154
	msm8940	1156
	msm8953	1157
	msm8996au	1162
	pm8937	1166
	pmp8074	1167
	qca1062	1168
	qca1064	1168
	qca4020	1169
	qca4024	1172
	qca6174a	1173
	qca6175a	1178
	qca6310	1181
	qca6320	1185
	qca6335	1188
	qca6390	1191
	qca6391	1199
	qca6420	1207

Vendor	Product	Page Number
Qualcomm	qca6421	1214
	qca6426	1218
	qca6428	1225
	qca6430	1226
	qca6431	1233
	qca6436	1236
	qca6438	1244
	qca6564	1244
	qca6564a	1246
	qca6564au	1251
	qca6574	1254
	qca6574a	1263
	qca6574au	1270
	qca6584	1277
	qca6595	1279
	qca6595au	1281
	qca6694	1288
	qca6696	1289
	qca8072	1295
	qca8075	1296
	qca8081	1296
	qca8337	1301
	qca9367	1305
	qca9377	1308
	qca9379	1313
	qca9888	1317
	qca9889	1317
	qcm2290	1317
	qcm4290	1323
	qcm6125	1329
	qcm6490	1331
	qcn5021	1337

Vendor	Product	Page Number
Qualcomm	qcs4290	1360
	qcs603	1366
	qcs605	1371
	qcs610	1376
	qcs6125	1380
	qcs6490	1382
	qrb5165	1388
	qrb5165m	1392
	qrb5165n	1396
	qsm8350	1400
	qualcomm215	1402
	sa415m	1408
	sa515m	1411
	sa6145p	1413
	sa6155	1417
	sa6155p	1422
	sa8155	1428
	sa8155p	1433
	sa8195p	1438
	sc8180x\+sdx55	1444
	sd429	1446
	sd439	1451
	sd450	1457
	sd460	1460
	sd480	1467
	sd632	1472
	sd660	1476
	sd662	1481
	sd665	1487
	sd670	1491
	sd675	1496
	sd678	1501

Vendor	Product	Page Number
Qualcomm	sd680	1507
	sd690_5g	1513
	sd695	1519
	sd710	1523
	sd712	1528
	sd720g	1530
	sd730	1535
	sd750g	1540
	sd765	1547
	sd765g	1554
	sd768	1561
	sd768g	1561
	sd778	1568
	sd778g	1569
	sd780	1575
	sd780g	1575
	sd7c	1582
	sd820	1583
	sd835	1585
	sd845	1589
	sd850	1592
	sd855	1593
	sd865_5g	1600
	sd870	1608
	sd888	1616
	sd888_5g	1622
	sdm429w	1630
	sdm630	1634
	sdw2500	1637
	sdx12	1640
	sdx20	1642
	sdx24	1645

Vendor	Product	Page Number
Qualcomm	sdx50m	1648
	sdx55	1652
	sdx55m	1658
	sdx65	1666
	sdxr1	1670
	sdxr2_5g	1674
	sd_636	1682
	sd_675	1685
	sd_8cx	1691
	sd_8cx_gen2	1693
	sd_8cx_gen3	1696
	sd_8_gen1_5g	1697
	sm4125	1706
	sm6250	1711
	sm6250p	1716
	sm7250p	1720
	sm7315	1728
	sm7325p	1734
	sm7450	1740
	sm8475	1749
	sm8475p	1756
	sw5100	1764
	sw5100p	1770
	wcd9326	1776
	wcd9330	1784
	wcd9335	1786
	wcd9340	1794
	wcd9341	1799
	wcd9360	1808
	wcd9370	1810
	wcd9371	1819
	wcd9375	1823

Vendor	Product	Page Number
Qualcomm	wcd9380	1832
	wcd9385	1841
	wcn3610	1850
	wcn3615	1853
	wcn3620	1860
	wcn3660	1864
	wcn3660b	1867
	wcn3680	1873
	wcn3680b	1878
	wcn3910	1884
	wcn3950	1890
	wcn3980	1896
	wcn3988	1905
	wcn3990	1912
	wcn3991	1919
	wcn3998	1927
	wcn3999	1936
	wcn6740	1940
	wcn6750	1946
	wcn6850	1955
	wcn6851	1964
	wcn6855	1972
	wcn6856	1981
	wcn7850	1990
	wcn7851	1996
	wsa8810	2005
	wsa8815	2014
	wsa8830	2023
	wsa8832	2033
	wsa8835	2041
Realtek	rtl8195am	2050
Sony	playstation_4	2051

Vendor	Product	Page Number
Qualcomm	ipq6005_firmware	2474
	ipq6010_firmware	2475
	ipq6018_firmware	2475
	ipq6028_firmware	2475
	ipq8070a_firmware	2476
	ipq8070_firmware	2476
	ipq8071a_firmware	2476
	ipq8071_firmware	2476
	ipq8072a_firmware	2477
	ipq8072_firmware	2477
	ipq8074a_firmware	2477
	ipq8074_firmware	2478
	ipq8076a_firmware	2478
	ipq8076_firmware	2478
	ipq8078a_firmware	2478
	ipq8078_firmware	2479
	ipq8173_firmware	2479
	ipq8174_firmware	2479
	mdm9150_firmware	2480
	mdm9206_firmware	2482
	mdm9250_firmware	2484
	mdm9607_firmware	2487
	mdm9626_firmware	2491
	mdm9628_firmware	2495
	mdm9640_firmware	2499
	mdm9650_firmware	2501
	msm8909w_firmware	2506
	msm8917_firmware	2509
	msm8920_firmware	2513
	msm8937_firmware	2513
	msm8940_firmware	2515
	msm8953_firmware	2516

Vendor	Product	Page Number
Qualcomm	msm8996au_firmware	2521
	pm8937_firmware	2525
	pmp8074_firmware	2526
	qca1062_firmware	2527
	qca1064_firmware	2527
	qca4020_firmware	2528
	qca4024_firmware	2531
	qca6174a_firmware	2532
	qca6175a_firmware	2537
	qca6310_firmware	2540
	qca6320_firmware	2544
	qca6335_firmware	2547
	qca6390_firmware	2550
	qca6391_firmware	2558
	qca6420_firmware	2566
	qca6421_firmware	2573
	qca6426_firmware	2577
	qca6428_firmware	2584
	qca6430_firmware	2585
	qca6431_firmware	2592
	qca6436_firmware	2595
	qca6438_firmware	2603
	qca6564au_firmware	2603
	qca6564a_firmware	2608
	qca6564_firmware	2613
	qca6574au_firmware	2616
	qca6574a_firmware	2623
	qca6574_firmware	2630
	qca6584_firmware	2636
	qca6595au_firmware	2638
	qca6595_firmware	2645
	qca6694_firmware	2647

Vendor	Product	Page Number
Qualcomm	qca6696_firmware	2648
	qca8072_firmware	2654
	qca8075_firmware	2655
	qca8081_firmware	2655
	qca8337_firmware	2660
	qca9367_firmware	2664
	qca9377_firmware	2667
	qca9379_firmware	2672
	qca9888_firmware	2676
	qca9889_firmware	2676
	qcm2290_firmware	2677
	qcm4290_firmware	2682
	qcm6125_firmware	2688
	qcm6490_firmware	2690
	qcn5021_firmware	2696
	qcn5022_firmware	2696
	qcn5024_firmware	2697
	qcn5052_firmware	2697
	qcn5054_firmware	2697
	qcn5064_firmware	2697
	qcn5121_firmware	2698
	qcn5122_firmware	2698
	qcn5124_firmware	2698
	qcn5152_firmware	2699
	qcn5154_firmware	2699
	qcn5164_firmware	2699
	qcn5550_firmware	2699
	qcn6023_firmware	2700
	qcn6024_firmware	2700
	qcn6100_firmware	2700
	qcn6102_firmware	2701
	qcn6112_firmware	2701

Vendor	Product	Page Number
Qualcomm	qcn6122_firmware	2701
	qcn6132_firmware	2701
	qcn7605_firmware	2702
	qcn7606_firmware	2703
	qcn9000_firmware	2704
	qcn9012_firmware	2705
	qcn9022_firmware	2705
	qcn9024_firmware	2705
	qcn9070_firmware	2706
	qcn9072_firmware	2706
	qcn9074_firmware	2706
	qcn9100_firmware	2706
	qcs2290_firmware	2707
	qcs405_firmware	2712
	qcs410_firmware	2716
	qcs4290_firmware	2719
	qcs603_firmware	2725
	qcs605_firmware	2730
	qcs610_firmware	2735
	qcs6125_firmware	2739
	qcs6490_firmware	2742
	qrb5165m_firmware	2747
	qrb5165n_firmware	2751
	qrb5165_firmware	2755
	qsm8350_firmware	2759
	qualcomm215_firmware	2761
	sa415m_firmware	2767
	sa515m_firmware	2770
	sa6145p_firmware	2772
	sa6155p_firmware	2776
	sa6155_firmware	2782
	sa8155p_firmware	2787

Vendor	Product	Page Number
Qualcomm	sa8155_firmware	2793
	sa8195p_firmware	2798
	sc8180x\+sdx55_firmware	2804
	sd429_firmware	2806
	sd439_firmware	2811
	sd450_firmware	2816
	sd460_firmware	2819
	sd480_firmware	2826
	sd632_firmware	2831
	sd660_firmware	2835
	sd662_firmware	2840
	sd665_firmware	2846
	sd670_firmware	2850
	sd675_firmware	2855
	sd678_firmware	2860
	sd680_firmware	2866
	sd690_5g_firmware	2872
	sd695_firmware	2878
	sd710_firmware	2882
	sd712_firmware	2887
	sd720g_firmware	2889
	sd730_firmware	2894
	sd750g_firmware	2899
	sd765g_firmware	2906
	sd765_firmware	2912
	sd768g_firmware	2920
	sd768_firmware	2927
	sd778g_firmware	2927
	sd778_firmware	2933
	sd780g_firmware	2934
	sd780_firmware	2940
	sd7c_firmware	2941

Vendor	Product	Page Number
Qualcomm	sd820_firmware	2942
	sd835_firmware	2944
	sd845_firmware	2948
	sd850_firmware	2951
	sd855_firmware	2952
	sd865_5g_firmware	2959
	sd870_firmware	2967
	sd888_5g_firmware	2975
	sd888_firmware	2983
	sdm429w_firmware	2989
	sdm630_firmware	2993
	sdw2500_firmware	2996
	sdx12_firmware	3000
	sdx20_firmware	3001
	sdx24_firmware	3004
	sdx50m_firmware	3007
	sdx55m_firmware	3011
	sdx55_firmware	3019
	sdx65_firmware	3025
	sdxr1_firmware	3029
	sdxr2_5g_firmware	3033
	sd_636_firmware	3041
	sd_675_firmware	3044
	sd_8cx_firmware	3050
	sd_8cx_gen2_firmware	3052
	sd_8cx_gen3_firmware	3055
	sd_8_gen1_5g_firmware	3056
	sm4125_firmware	3065
	sm6250p_firmware	3070
	sm6250_firmware	3074
	sm7250p_firmware	3079
	sm7315_firmware	3087

Vendor	Product	Page Number
Qualcomm	sm7325p_firmware	3093
	sm7450_firmware	3099
	sm8475p_firmware	3108
	sm8475_firmware	3115
	sw5100p_firmware	3123
	sw5100_firmware	3129
	wcd9326_firmware	3135
	wcd9330_firmware	3143
	wcd9335_firmware	3145
	wcd9340_firmware	3153
	wcd9341_firmware	3158
	wcd9360_firmware	3167
	wcd9370_firmware	3169
	wcd9371_firmware	3178
	wcd9375_firmware	3182
	wcd9380_firmware	3191
	wcd9385_firmware	3200
	wcn3610_firmware	3209
	wcn3615_firmware	3212
	wcn3620_firmware	3219
	wcn3660b_firmware	3223
	wcn3660_firmware	3229
	wcn3680b_firmware	3232
	wcn3680_firmware	3238
	wcn3910_firmware	3243
	wcn3950_firmware	3249
	wcn3980_firmware	3256
	wcn3988_firmware	3264
	wcn3990_firmware	3271
	wcn3991_firmware	3278
	wcn3998_firmware	3286
	wcn3999_firmware	3295

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10-strike					
Product: network_inventory_explorer					
Affected Version(s): * Up to (including) 9.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-Sep-2022	9.8	10-Strike Network Inventory Explorer v9.3 was discovered to contain a buffer overflow via the Add Computers function. **CVE ID : CVE-2022-38573**	N/A	A-10--NETW-101022/1
Vendor: 10up					
Product: restricted_site_access					
Affected Version(s): * Up to (excluding) 7.3.2					
Authorization Bypass Through User-Controlled Key	26-Sep-2022	5.3	The Restricted Site Access WordPress plugin before 7.3.2 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based limitations in certain situations. **CVE ID : CVE-2022-1613**	https://wpscan.com/vulnerability/c03863ef-9ac9-402b-8f8d-9559c9988e2b	A-10U-REST-101022/2
Vendor: 3d_tag_cloud_project					
Product: 3d_tag_cloud					
Affected Version(s): * Up to (including) 3.8					
Cross-Site Request	23-Sep-2022	6.1	Multiple Stored Cross-Site Scripting	https://wordpress.org/plugins	A-3D_-3D_T-101022/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			(XSS) via Cross-Site Request Forgery (CSRF) vulnerability in 3D Tag Cloud plugin <= 3.8 at WordPress. **CVE ID : CVE-2022-36417**	/cardoza-3d-tag-cloud/, https://patchstack.com/database/vulnerability/cardoza-3d-tag-cloud/wordpress-3d-tag-cloud-plugin-3-8-multiple-stored-cross-site-scripting-xss-via-cross-site-request-forgery-csrf-vulnerability/_s_id=cve	
Vendor: acnam					
Product: wp_server_health_stats					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	4.8	The WP Server Health Stats WordPress plugin before 1.7.0 does not escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-2887**	N/A	A-ACN-WP_S-101022/4
Vendor: add_shortcodes_actions_and_filters_project					
Product: add_shortcodes_actions_and_filters					
Affected Version(s): * Up to (including) 2.0.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	4.8	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability Add Shortcodes Actions And Filters plugin <= 2.0.9 at WordPress. **CVE ID : CVE-2022-37342**	https://patchstack.com/database/vulnerability/add-actions-and-filters/wordpress-add-shortcodes-actions-and-filters-plugin-2-0-9-authenticated-stored-cross-site-scripting-xss-vulnerability/_s_id=cve, https://wordpress.org/plugins/add-actions-and-filters/	A-ADD-ADD_-101022/5
Vendor: Adobe					
Product: animate					
Affected Version(s): From (including) 21.0 Up to (including) 21.0.11					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/animate/apsb22-54.html	A-ADO-ANIM-101022/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38411		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38412**	https://helpx.adobe.com/security/products/animate/apsb22-54.html	A-ADO-ANIM-101022/7
Affected Version(s): From (including) 22.0 Up to (including) 22.0.7					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/animate/apsb22-54.html	A-ADO-ANIM-101022/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38411**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38412**	https://helpx.adobe.com/security/products/animate/apsb22-54.html	A-ADO-ANIM-101022/9
Product: bridge					
Affected Version(s): From (including) 11.1 Up to (excluding) 11.1.4					
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35699**		
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35700**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/11
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35701**		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35702**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/13
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35703**		
Use After Free	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35704**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/15
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35705**		
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35706**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/17
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35707**		
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35708**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/19
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3	https://helpx.adobe.com/security/products/br	A-ADO-BRID-101022/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35709**	idge/apsb22-49.html	
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38425**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/21
Affected Version(s): From (including) 12.0 Up to (excluding) 12.0.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35699**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/22
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35700**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/23
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-	https://helpx.adobe.com/security/products/br	A-ADO-BRID-101022/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35701**	idge/apsb22-49.html	
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35702**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35703**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/26
Use After Free	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35704		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35705**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/28
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35706**		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35707**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/30
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35708**		
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35709**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/32
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	A-ADO-BRID-101022/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38425**		
Product: download_manager					
Affected Version(s): * Up to (excluding) 3.2.55					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-Sep-2022	4.9	The Download Manager WordPress plugin before 3.2.55 does not validate one of its settings, which could allow high privilege users such as admin to list and read arbitrary files and folders outside of the blog directory **CVE ID : CVE-2022-2926**	N/A	A-ADO-DOWN-101022/34
Product: experience_manager					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30677**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30678**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/36
Improper Neutralization of Input During Web Page Generation	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30680**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30681**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/38
Improper Neutralization of	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and	https://helpx.adobe.com/security/products/ex	A-ADO-EXPE-101022/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30682**	perience-manager/apsb22-40.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM.	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30684		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30685**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/41
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30686**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-34218**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/43
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page,	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-35664**		
Inadequate Encryption Strength	16-Sep-2022	5.3	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a Violation of Secure Design Principles vulnerability that could lead to bypass the security feature of the encryption mechanism in the backend . An attacker could leverage this vulnerability to decrypt secrets, however, this is a high-complexity attack as the threat actor needs to already possess those secrets. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30683**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 6.5.14.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-38438**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-38439**		
Affected Version(s): * Up to (including) 6.5.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30677**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/48
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30678**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30680**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/50
Improper Neutralization of Input During Web Page	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-101022/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			(XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30681**	manager/apsb22-40.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30682**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30684**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/53
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30685**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30686**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/55
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-34218**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-35664**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/57
Inadequate Encryption Strength	16-Sep-2022	5.3	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a Violation of Secure Design Principles vulnerability that could lead to	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the security feature of the encryption mechanism in the backend . An attacker could leverage this vulnerability to decrypt secrets, however, this is a high-complexity attack as the threat actor needs to already possess those secrets. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-30683**		
Product: experience_manager_cloud_service					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege access to AEM. **CVE ID : CVE-2022-38438**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Adobe Experience Manager versions 6.5.13.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires low-privilege access to AEM. **CVE ID : CVE-2022-38439**	https://helpx.adobe.com/security/products/experience-manager/apsb22-40.html	A-ADO-EXPE-101022/60
Product: illustrator					
Affected Version(s): From (including) 25.0 Up to (including) 25.4.7					
Improper Input Validation	16-Sep-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	A-ADO-ILLU-101022/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38408**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38409**	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	A-ADO-ILLU-101022/62
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	A-ADO-ILLU-101022/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38410**		
Affected Version(s): From (including) 26.0 Up to (including) 26.4					
Improper Input Validation	16-Sep-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38408**	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	A-ADO-ILLU-101022/64
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are	https://helpx.adobe.com/security/products/ill	A-ADO-ILLU-101022/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38409**	ustrator/apsb22-55.html	
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38410**	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	A-ADO-ILLU-101022/66
Product: incopy					
Affected Version(s): From (including) 16.0 Up to (including) 16.4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38401**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/67
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38402**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38403**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/69
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38404**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38405**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/71
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38406**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38407**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/73
Affected Version(s): From (including) 17.0 Up to (including) 17.3					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38401		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38402**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/75
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38403**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38404**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/77
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38405**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38406**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/79
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	A-ADO-INCO-101022/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38407		
Product: indesign					
Affected Version(s): From (including) 16.0 Up to (including) 16.4.2					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28852**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/81
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28853**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38413**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/83
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38414**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38415**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/85
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-38416**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38417**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/87
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28854**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28855**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/89
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28856**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28857**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/91
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30671**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30672**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/93
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30673**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30674**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/95
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30675**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30676**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/97
Affected Version(s): From (including) 17.0 Up to (including) 17.3					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by by an out-of-bounds	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28852**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28853**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/99
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38413**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38414**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/101
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38415**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38416**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/103
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38417**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28854**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/105
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28855**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28856**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/107
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an	https://helpx.adobe.com/security/products/in	A-ADO-INDE-101022/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28857**	design/apsb22-50.html	
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30671**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/109
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier)	https://helpx.adobe.com/security/products/in	A-ADO-INDE-101022/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30672**	design/apsb22-50.html	
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30673**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30674**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/112
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30675		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30676**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	A-ADO-INDE-101022/114
Product: photoshop					
Affected Version(s): From (including) 22.0 Up to (including) 22.5.8					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-35713**		
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38426**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/116
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-38427**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38429**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/118
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38430**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38431**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/120
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier)	https://helpx.adobe.com/security/products/p	A-ADO-PHOT-101022/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38432**	hotoshop/apsb22-52.html	
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.sue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38433**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/122
Use After Free	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and	https://helpx.adobe.com/security/products/p	A-ADO-PHOT-101022/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.4.2 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38434**	hotoshop/apsb22-52.html	
Use After Free	16-Sep-2022	5.5	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38428**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/124
Affected Version(s): From (including) 23.0 Up to (including) 23.4.2					
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and	https://helpx.adobe.com/security/products/p	A-ADO-PHOT-101022/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.4.2 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35713**	hotoshop/apsb22-52.html	
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38426**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/126
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38427**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38429**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38430**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/129
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38431**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38432**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/131
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file.sue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38433**		
Use After Free	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38434**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/133
Use After Free	16-Sep-2022	5.5	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	A-ADO-PHOT-101022/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38428**		
Vendor: Advantech					
Product: iview					
Affected Version(s): 5.7.04.6469					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-2022	7.5	An SQL injection vulnerability in Advantech iView 5.7.04.6469. The specific flaw exists within the ConfigurationServlet endpoint, which listens on TCP port 8080 by default. An unauthenticated remote attacker can craft a special column_value parameter in the setConfiguration action to bypass checks in com.imc.iview.utils.CUtils.checkSQLInjection() to perform SQL injection. For example, the attacker can exploit the vulnerability to retrieve the iView admin password. **CVE ID : CVE-2022-3323**	N/A	A-ADV-IVIE-101022/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ahsay					
Product: cloud_backup_suite					
Affected Version(s): 9.1.4.0					
N/A	21-Sep-2022	7.2	Ahsay AhsayCBS 9.1.4.0 allows an authenticated system user to inject arbitrary Java JVM options. Administrators that can modify the Runtime Options in the web interface can inject Java Runtime Options. These take effect after a restart. For example, an attacker can enable JMX services and consequently achieve remote code execution as the system user. **CVE ID : CVE-2022-37027**	https://wiki.ahsay.com/doku.php?id=public:resources:release_notes_v9320, https://www.ahsay.com/jsp/en/downloads/ahsay-downloads_latest-software_ahsaycbs.jsp, https://www.ahsay.com/partners/en/home/index.jsp?pageContentKey=ahsay_assets_latest_hotfix	A-AHS-CLOU-101022/136
Vendor: Ajaxplorer					
Product: ajaxplorer					
Affected Version(s): 4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	An issue was discovered in AjaXplorer 4.2.3, allows attackers to cause cross site scripting vulnerabilities via a crafted svg file upload. **CVE ID : CVE-2022-40358**	N/A	A-AJA-AJAX-101022/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: algolplus					
Product: advanced_dynamic_pricing_for_woocommerce					
Affected Version(s): * Up to (including) 4.1.3					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in AlgolPlus Advanced Dynamic Pricing for WooCommerce plugin <= 4.1.3 at WordPress. **CVE ID : CVE-2022-38095**	https://patchstack.com/database/vulnerability/advanced-dynamic-pricing-for-woocommerce/wordpress-advanced-dynamic-pricing-for-woocommerce-plugin-4-1-3-cross-site-request-forgery-csrf-vulnerability	A-ALG-ADVA-101022/138
Vendor: Amazon					
Product: fhir-works-on-aws-authz-smart					
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.3					
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-2022	6.5	fhir-works-on-aws-authz-smart is an implementation of the authorization interface from the FHIR Works interface. Versions 3.1.1 and 3.1.2 are subject to Exposure of Sensitive Information to an Unauthorized Actor. This issue allows a client of the API to retrieve more information than the client's OAuth scope	https://github.com/awslabs/fhir-works-on-aws-authz-smart/security/advisories/GHSA-vv7x-7w4m-q72f	A-AMA-FHIR-101022/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permits when making "search-type" requests. This issue would not allow a client to retrieve information about individuals other than those the client was already authorized to access. Users of fhir-works-on-aws-authz-smart 3.1.1 or 3.1.2 should upgrade to version 3.1.3 or higher immediately. Versions 3.1.0 and below are unaffected. There is no workaround for this issue. **CVE ID : CVE-2022-39230**		
Vendor: Apache					
Product: airflow					
Affected Version(s): From (including) 2.3.0 Up to (including) 2.3.4					
Use of Externally-Controlled Format String	21-Sep-2022	7.5	In Apache Airflow 2.3.0 through 2.3.4, part of a url was unnecessarily formatted, allowing for possible information extraction. **CVE ID : CVE-2022-40604**	https://lists.apache.org/thread/z20x8m16fnhxdkoollv53w1ybsts687t, https://github.com/apache/airflow/pull/26337	A-APA-AIRF-101022/140
URL Redirection to Untrusted	21-Sep-2022	6.1	In Apache Airflow 2.3.0 through 2.3.4, there was an open redirect in the	https://github.com/apache/airflow/pull/26409,	A-APA-AIRF-101022/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			webserver's `/confirm` endpoint. **CVE ID : CVE-2022-40754**	https://lists.apache.org/thread/cn098dcp5x3c402xrb06p3l7nz5goffm	
Product: batik					
Affected Version(s): 1.14					
Server-Side Request Forgery (SSRF)	22-Sep-2022	7.5	Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to access files using a Jar url. This issue affects Apache XML Graphics Batik 1.14. **CVE ID : CVE-2022-40146**	https://lists.apache.org/thread/hxtddqjty2sbs12y97c8g7xfh17jzxsx	A-APA-BATI-101022/142
Server-Side Request Forgery (SSRF)	22-Sep-2022	5.3	Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache XML Graphics allows an attacker to load a url thru the jar protocol. This issue affects Apache XML Graphics Batik 1.14. **CVE ID : CVE-2022-38398**	https://lists.apache.org/thread/712c9xwtmyghyokzrm2ml6sps4xlmbsx	A-APA-BATI-101022/143
Server-Side Request Forgery (SSRF)	22-Sep-2022	5.3	Server-Side Request Forgery (SSRF) vulnerability in Batik of Apache	https://lists.apache.org/thread/gfsktxvj7jtwyovmhhbrw0bs13wfjd7b	A-APA-BATI-101022/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XML Graphics allows an attacker to fetch external resources. This issue affects Apache XML Graphics Batik 1.14. **CVE ID : CVE-2022-38648**		
Product: inlong					
Affected Version(s): * Up to (excluding) 1.3.0					
Deserialization of Untrusted Data	20-Sep-2022	8.8	In versions of Apache InLong prior to 1.3.0, an attacker with sufficient privileges to specify MySQL JDBC connection URL parameters and to write arbitrary data to the MySQL database, could cause this data to be deserialized by Apache InLong, potentially leading to Remote Code Execution on the Apache InLong server. Users are advised to upgrade to Apache InLong 1.3.0 or newer. **CVE ID : CVE-2022-40955**	https://lists.apache.org/thread/r1r34y7bchrpmp9jhfdoohzdmk7pj1q1	A-APA-INLO-101022/145
Product: kafka					
Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	20-Sep-2022	7.5	A security vulnerability has been identified in Apache Kafka. It affects all releases since 2.8.0. The vulnerability allows malicious unauthenticated clients to allocate large amounts of memory on brokers. This can lead to brokers hitting OutOfMemoryException and causing denial of service. Example scenarios: - Kafka cluster without authentication: Any clients able to establish a network connection to a broker can trigger the issue. - Kafka cluster with SASL authentication: Any clients able to establish a network connection to a broker, without the need for valid SASL credentials, can trigger the issue. - Kafka cluster with TLS authentication: Only clients able to successfully authenticate via TLS can trigger the issue. We advise the users to	https://kafka.apache.org/cve-list	A-APA-KAFK-101022/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the Kafka installations to one of the 3.2.3, 3.1.2, 3.0.2, 2.8.2 versions. **CVE ID : CVE-2022-34917**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.2					
Allocation of Resources Without Limits or Throttling	20-Sep-2022	7.5	A security vulnerability has been identified in Apache Kafka. It affects all releases since 2.8.0. The vulnerability allows malicious unauthenticated clients to allocate large amounts of memory on brokers. This can lead to brokers hitting OutOfMemoryException and causing denial of service. Example scenarios: - Kafka cluster without authentication: Any clients able to establish a network connection to a broker can trigger the issue. - Kafka cluster with SASL authentication: Any clients able to establish a network connection to a broker, without the need for valid SASL credentials, can	https://kafka.apache.org/cve-list	A-APA-KAFK-101022/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger the issue. - Kafka cluster with TLS authentication: Only clients able to successfully authenticate via TLS can trigger the issue. We advise the users to upgrade the Kafka installations to one of the 3.2.3, 3.1.2, 3.0.2, 2.8.2 versions. **CVE ID : CVE-2022-34917**		
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.1.2					
Allocation of Resources Without Limits or Throttling	20-Sep-2022	7.5	A security vulnerability has been identified in Apache Kafka. It affects all releases since 2.8.0. The vulnerability allows malicious unauthenticated clients to allocate large amounts of memory on brokers. This can lead to brokers hitting OutOfMemoryException and causing denial of service. Example scenarios: - Kafka cluster without authentication: Any clients able to establish a network connection to a broker can trigger	https://kafka.apache.org/cve-list	A-APA-KAFK-101022/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue. - Kafka cluster with SASL authentication: Any clients able to establish a network connection to a broker, without the need for valid SASL credentials, can trigger the issue. - Kafka cluster with TLS authentication: Only clients able to successfully authenticate via TLS can trigger the issue. We advise the users to upgrade the Kafka installations to one of the 3.2.3, 3.1.2, 3.0.2, 2.8.2 versions. **CVE ID : CVE-2022-34917**		
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.2.3					
Allocation of Resources Without Limits or Throttling	20-Sep-2022	7.5	A security vulnerability has been identified in Apache Kafka. It affects all releases since 2.8.0. The vulnerability allows malicious unauthenticated clients to allocate large amounts of memory on brokers. This can lead to brokers hitting OutOfMemoryException and causing	https://kafka.apache.org/cve-list	A-APA-KAFK-101022/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			denial of service. Example scenarios: - Kafka cluster without authentication: Any clients able to establish a network connection to a broker can trigger the issue. - Kafka cluster with SASL authentication: Any clients able to establish a network connection to a broker, without the need for valid SASL credentials, can trigger the issue. - Kafka cluster with TLS authentication: Only clients able to successfully authenticate via TLS can trigger the issue. We advise the users to upgrade the Kafka installations to one of the 3.2.3, 3.1.2, 3.0.2, 2.8.2 versions. **CVE ID : CVE-2022-34917**		
Product: pinot					
Affected Version(s): * Up to (excluding) 0.11.0					
N/A	23-Sep-2022	9.8	In 0.10.0 or older versions of Apache Pinot, Pinot query endpoint and realtime ingestion layer has a vulnerability in	https://lists.apache.org/thread/4pb0r12s2b68d78llk04yd8rh3qk5t9h	A-APA-PINO-101022/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unprotected environments due to a groovy function support. In order to avoid this, we disabled the groovy function support by default from Pinot release 0.11.0. See https://docs.pinot.apache.org/basics/releases/0.11.0 **CVE ID : CVE-2022-26112**		
Product: pulsar					
Affected Version(s): * Up to (excluding) 2.7.5					
Improper Certificate Validation	23-Sep-2022	5.9	Delayed TLS hostname verification in the Pulsar Java Client and the Pulsar Proxy make each client vulnerable to a man in the middle attack. Connections from the Pulsar Java Client to the Pulsar Broker/Proxy and connections from the Pulsar Proxy to the Pulsar Broker are vulnerable. Authentication data is sent before verifying the server's TLS certificate matches the hostname, which means authentication data could be exposed	https://lists.apache.org/thread/fpo6x10trvn20hlk0dmnr5vlz5v4kl3d	A-APA-PULS-101022/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to an attacker. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. Because the client sends authentication data before performing hostname verification, an attacker could gain access to the client's authentication data. The client eventually closes the connection when it verifies the hostname and identifies the targeted hostname does not match a hostname on the certificate. Because the client eventually closes the connection, the value of the intercepted authentication data depends on the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication method used by the client. Token based authentication and username/password authentication methods are vulnerable because the authentication data can be used to impersonate the client in a separate session. This issue affects Apache Pulsar Java Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33681**		
Improper Certificate Validation	23-Sep-2022	5.9	TLS hostname verification cannot be enabled in the Pulsar Broker's Java Client, the Pulsar Broker's Java Admin Client, the Pulsar WebSocket Proxy's Java Client, and the Pulsar Proxy's Admin Client leaving intra-cluster connections and geo-replication connections vulnerable to man in the middle attacks, which could leak	https://lists.apache.org/thread/l0ynfl161qghwfcgbbl8ld9hzbl9t3yx	A-APA-PULS-101022/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials, configuration data, message data, and any other data sent by these clients. The vulnerability is for both the pulsar+ssl protocol and HTTPS. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. This issue affects Apache Pulsar Broker, Proxy, and WebSocket Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33682**		
Improper Certificate Validation	23-Sep-2022	5.9	Apache Pulsar Brokers and Proxies create an internal Pulsar Admin Client that does not verify peer TLS	https://lists.apache.org/thread/42v5rsxj36r3nhfxhmhb2x12r5jmvx3x	A-APA-PULS-101022/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certificates, even when tlsAllowInsecureConnection is disabled via configuration. The Pulsar Admin Client's intra-cluster and geo-replication HTTPS connections are vulnerable to man in the middle attacks, which could leak authentication data, configuration data, and any other data sent by these clients. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. This issue affects Apache Pulsar Broker and Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33683**		
Affected Version(s): * Up to (including) 2.6.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Sep-2022	6.5	Improper Input Validation vulnerability in Proxy component of Apache Pulsar allows an attacker to make TCP/IP connection attempts that originate from the Pulsar Proxy's IP address. When the Apache Pulsar Proxy component is used, it is possible to attempt to open TCP/IP connections to any IP address and port that the Pulsar Proxy can connect to. An attacker could use this as a way for DoS attacks that originate from the Pulsar Proxy's IP address. It hasn't been detected that the Pulsar Proxy authentication can be bypassed. The attacker will have to have a valid token to a properly secured Pulsar Proxy. This issue affects Apache Pulsar Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.2; 2.9.0 to 2.9.1; 2.6.4 and earlier.	https://lists.apache.org/thread/ghs9jtjfbpy4c6xcftyvkl6swznlom1v	A-APA-PULS-101022/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24280		
Affected Version(s): 2.10.0					
Improper Certificate Validation	23-Sep-2022	5.9	Delayed TLS hostname verification in the Pulsar Java Client and the Pulsar Proxy make each client vulnerable to a man in the middle attack. Connections from the Pulsar Java Client to the Pulsar Broker/Proxy and connections from the Pulsar Proxy to the Pulsar Broker are vulnerable. Authentication data is sent before verifying the server's TLS certificate matches the hostname, which means authentication data could be exposed to an attacker. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a	https://lists.apache.org/thread/fpo6x10trvn20hlk0dmnr5vlz5v4kl3d	A-APA-PULS-101022/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cryptographically valid certificate for an unrelated host. Because the client sends authentication data before performing hostname verification, an attacker could gain access to the client's authentication data. The client eventually closes the connection when it verifies the hostname and identifies the targeted hostname does not match a hostname on the certificate. Because the client eventually closes the connection, the value of the intercepted authentication data depends on the authentication method used by the client. Token based authentication and username/password authentication methods are vulnerable because the authentication data can be used to impersonate the client in a separate session. This issue		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Apache Pulsar Java Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33681**		
Improper Certificate Validation	23-Sep-2022	5.9	TLS hostname verification cannot be enabled in the Pulsar Broker's Java Client, the Pulsar Broker's Java Admin Client, the Pulsar WebSocket Proxy's Java Client, and the Pulsar Proxy's Admin Client leaving intra-cluster connections and geo-replication connections vulnerable to man in the middle attacks, which could leak credentials, configuration data, message data, and any other data sent by these clients. The vulnerability is for both the pulsar+ssl protocol and HTTPS. An attacker can only take advantage of this vulnerability by taking control of a machine	https://lists.apache.org/thread/l0ynfl161qghwfcgbbl8ld9hzbl9t3yx	A-APA-PULS-101022/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. This issue affects Apache Pulsar Broker, Proxy, and WebSocket Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33682**		
Improper Certificate Validation	23-Sep-2022	5.9	Apache Pulsar Brokers and Proxies create an internal Pulsar Admin Client that does not verify peer TLS certificates, even when tlsAllowInsecureConnection is disabled via configuration. The Pulsar Admin Client's intra-cluster and geo-replication HTTPS connections are vulnerable to man in the middle attacks, which	https://lists.apache.org/thread/42v5rsxj36r3nhfxhmhb2x12r5jmvx3x	A-APA-PULS-101022/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leak authentication data, configuration data, and any other data sent by these clients. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. This issue affects Apache Pulsar Broker and Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33683**		
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.7.5					
Improper Input Validation	23-Sep-2022	6.5	Improper Input Validation vulnerability in Proxy component of Apache Pulsar allows an attacker to make TCP/IP connection attempts that originate from the Pulsar Proxy's IP address. When the Apache Pulsar Proxy component is used, it is	https://lists.apache.org/thread/ghs9jtjfbpy4c6xcftyvkl6swznlom1v	A-APA-PULS-101022/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to attempt to open TCP/IP connections to any IP address and port that the Pulsar Proxy can connect to. An attacker could use this as a way for DoS attacks that originate from the Pulsar Proxy's IP address. It hasn't been detected that the Pulsar Proxy authentication can be bypassed. The attacker will have to have a valid token to a properly secured Pulsar Proxy. This issue affects Apache Pulsar Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.2; 2.9.0 to 2.9.1; 2.6.4 and earlier. **CVE ID : CVE-2022-24280**		
Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.3					
Improper Input Validation	23-Sep-2022	6.5	Improper Input Validation vulnerability in Proxy component of Apache Pulsar allows an attacker to make TCP/IP connection attempts that originate from the Pulsar Proxy's IP address. When the	https://lists.apache.org/thread/ghs9jtjfbpy4c6xcftyvkl6swznlom1v	A-APA-PULS-101022/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Apache Pulsar Proxy component is used, it is possible to attempt to open TCP/IP connections to any IP address and port that the Pulsar Proxy can connect to. An attacker could use this as a way for DoS attacks that originate from the Pulsar Proxy's IP address. It hasn't been detected that the Pulsar Proxy authentication can be bypassed. The attacker will have to have a valid token to a properly secured Pulsar Proxy. This issue affects Apache Pulsar Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.2; 2.9.0 to 2.9.1; 2.6.4 and earlier. **CVE ID : CVE-2022-24280**		
Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.4					
Improper Certificate Validation	23-Sep-2022	5.9	Delayed TLS hostname verification in the Pulsar Java Client and the Pulsar Proxy make each client vulnerable to a man in the middle attack.	https://lists.apache.org/thread/fpo6x10trvn20hlk0dmnr5vlz5v4kl3d	A-APA-PULS-101022/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connections from the Pulsar Java Client to the Pulsar Broker/Proxy and connections from the Pulsar Proxy to the Pulsar Broker are vulnerable. Authentication data is sent before verifying the server's TLS certificate matches the hostname, which means authentication data could be exposed to an attacker. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. Because the client sends authentication data before performing hostname verification, an attacker could gain access to the client's authentication		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data. The client eventually closes the connection when it verifies the hostname and identifies the targeted hostname does not match a hostname on the certificate. Because the client eventually closes the connection, the value of the intercepted authentication data depends on the authentication method used by the client. Token based authentication and username/password authentication methods are vulnerable because the authentication data can be used to impersonate the client in a separate session. This issue affects Apache Pulsar Java Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33681**		
Improper Certificate Validation	23-Sep-2022	5.9	TLS hostname verification cannot be enabled in the	https://lists.apache.org/thread/l0ynfl161qghwf	A-APA-PULS-101022/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Pulsar Broker's Java Client, the Pulsar Broker's Java Admin Client, the Pulsar WebSocket Proxy's Java Client, and the Pulsar Proxy's Admin Client leaving intra-cluster connections and geo-replication connections vulnerable to man in the middle attacks, which could leak credentials, configuration data, message data, and any other data sent by these clients. The vulnerability is for both the pulsar+ssl protocol and HTTPS. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. This issue affects Apache Pulsar	cgbbl8ld9hzbl9t3yx	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Broker, Proxy, and WebSocket Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33682**		
Improper Certificate Validation	23-Sep-2022	5.9	Apache Pulsar Brokers and Proxies create an internal Pulsar Admin Client that does not verify peer TLS certificates, even when tlsAllowInsecureConnection is disabled via configuration. The Pulsar Admin Client's intra-cluster and geo-replication HTTPS connections are vulnerable to man in the middle attacks, which could leak authentication data, configuration data, and any other data sent by these clients. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The	https://lists.apache.org/thread/42v5rsxj36r3nhfxhmhb2x12r5jmvx3x	A-APA-PULS-101022/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker must then actively manipulate traffic to perform the attack. This issue affects Apache Pulsar Broker and Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33683**		
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.2					
Improper Input Validation	23-Sep-2022	6.5	Improper Input Validation vulnerability in Proxy component of Apache Pulsar allows an attacker to make TCP/IP connection attempts that originate from the Pulsar Proxy's IP address. When the Apache Pulsar Proxy component is used, it is possible to attempt to open TCP/IP connections to any IP address and port that the Pulsar Proxy can connect to. An attacker could use this as a way for DoS attacks that originate from the Pulsar Proxy's IP address. It hasn't	https://lists.apache.org/thread/ghs9jtjfbpy4c6xcftyvkl6swznlom1v	A-APA-PULS-101022/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been detected that the Pulsar Proxy authentication can be bypassed. The attacker will have to have a valid token to a properly secured Pulsar Proxy. This issue affects Apache Pulsar Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.2; 2.9.0 to 2.9.1; 2.6.4 and earlier. **CVE ID : CVE-2022-24280**		
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.3					
Improper Certificate Validation	23-Sep-2022	5.9	Delayed TLS hostname verification in the Pulsar Java Client and the Pulsar Proxy make each client vulnerable to a man in the middle attack. Connections from the Pulsar Java Client to the Pulsar Broker/Proxy and connections from the Pulsar Proxy to the Pulsar Broker are vulnerable. Authentication data is sent before verifying the server's TLS certificate matches the hostname, which means authentication data	https://lists.apache.org/thread/fpo6x10trvn20hlk0dmnr5vlz5v4kl3d	A-APA-PULS-101022/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be exposed to an attacker. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. Because the client sends authentication data before performing hostname verification, an attacker could gain access to the client's authentication data. The client eventually closes the connection when it verifies the hostname and identifies the targeted hostname does not match a hostname on the certificate. Because the client eventually closes the connection, the value of the intercepted authentication data		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			depends on the authentication method used by the client. Token based authentication and username/password authentication methods are vulnerable because the authentication data can be used to impersonate the client in a separate session. This issue affects Apache Pulsar Java Client versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33681**		
Improper Certificate Validation	23-Sep-2022	5.9	TLS hostname verification cannot be enabled in the Pulsar Broker's Java Client, the Pulsar Broker's Java Admin Client, the Pulsar WebSocket Proxy's Java Client, and the Pulsar Proxy's Admin Client leaving intra-cluster connections and geo-replication connections vulnerable to man in the middle attacks, which	https://lists.apache.org/thread/l0ynfl161qghwfcgbbl8ld9hzbl9t3yx	A-APA-PULS-101022/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could leak credentials, configuration data, message data, and any other data sent by these clients. The vulnerability is for both the pulsar+ssl protocol and HTTPS. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack by providing the client with a cryptographically valid certificate for an unrelated host. This issue affects Apache Pulsar Broker, Proxy, and WebSocket Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33682**		
Improper Certificate Validation	23-Sep-2022	5.9	Apache Pulsar Brokers and Proxies create an internal Pulsar Admin Client that does not verify	https://lists.apache.org/thread/42v5rsxj36r3nhfxhmhb2x12r5jmvx3x	A-APA-PULS-101022/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer TLS certificates, even when tlsAllowInsecureConnection is disabled via configuration. The Pulsar Admin Client's intra-cluster and geo-replication HTTPS connections are vulnerable to man in the middle attacks, which could leak authentication data, configuration data, and any other data sent by these clients. An attacker can only take advantage of this vulnerability by taking control of a machine 'between' the client and the server. The attacker must then actively manipulate traffic to perform the attack. This issue affects Apache Pulsar Broker and Proxy versions 2.7.0 to 2.7.4; 2.8.0 to 2.8.3; 2.9.0 to 2.9.2; 2.10.0; 2.6.4 and earlier. **CVE ID : CVE-2022-33683**		
Vendor: apasionados					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: export_post_info					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Formula Elements in a CSV File	23-Sep-2022	5.7	Authenticated (author+) CSV Injection vulnerability in Export Post Info plugin <= 1.2.0 at WordPress. **CVE ID : CVE-2022-38061**	https://wordpress.org/plugins/export-post-info/#developers, https://patchstack.com/database/vulnerability/export-post-info/wordpress-export-post-info-plugin-1-2-0-authenticated-csv-injection-vulnerability/_s_id=cve	A-APA-EXPO-101022/167
Vendor: Apple					
Product: itunes					
Affected Version(s): * Up to (excluding) 12.12.3					
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	A-APP-ITUN-101022/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22629		
Product: safari					
Affected Version(s): * Up to (excluding) 15.4					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-22610**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	A-APP-SAFA-101022/169
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4, tvOS 15.4, Safari 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22624**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	A-APP-SAFA-101022/170
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with	https://support.apple.com/en-us/HT213186,	A-APP-SAFA-101022/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22628**	https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22629**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	A-APP-SAFA-101022/172
N/A	23-Sep-2022	8.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-	A-APP-SAFA-101022/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior. **CVE ID : CVE-2022-22637**	us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Affected Version(s): * Up to (excluding) 15.5					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-26700**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	A-APP-SAFA-101022/174
Affected Version(s): * Up to (excluding) 15.6					
Out-of-bounds Write	20-Sep-2022	9.8	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 15.6, macOS Monterey 12.5. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213341	A-APP-SAFA-101022/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32863		
N/A	20-Sep-2022	5.3	A logic issue was addressed with improved state management. This issue is fixed in Safari 15.6, macOS Monterey 12.5. A user may be tracked through their IP address. **CVE ID : CVE-2022-32861**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213341	A-APP-SAFA-101022/176
Affected Version(s): * Up to (excluding) 16.0					
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32886**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	A-APP-SAFA-101022/177
Out-of-bounds Read	20-Sep-2022	8.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	A-APP-SAFA-101022/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32912**		
N/A	20-Sep-2022	4.3	A logic issue was addressed with improved state management. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. A website may be able to track users through Safari web extensions. **CVE ID : CVE-2022-32868**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	A-APP-SAFA-101022/179
Product: swift-nio-extras					
Affected Version(s): * Up to (excluding) 1.9.2					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Sep-2022	7.5	Improper detection of complete HTTP body decompression SwiftNIO Extras provides a pair of helpers for transparently decompressing received HTTP request or response bodies. These two objects (HTTPRequestDecompressor and HTTPResponseDecompressor) both failed to detect when the decompressed body was	N/A	A-APP-SWIF-101022/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			considered complete. If trailing junk data was appended to the HTTP message body, the code would repeatedly attempt to decompress this data and fail. This would lead to an infinite loop making no forward progress, leading to livelock of the system and denial-of-service. This issue can be triggered by any attacker capable of sending a compressed HTTP message. Most commonly this is HTTP servers, as compressed HTTP messages cannot be negotiated for HTTP requests, but it is possible that users have configured decompression for HTTP requests as well. The attack is low effort, and likely to be reached without requiring any privilege or system access. The impact on availability is high: the process immediately		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			becomes unavailable but does not immediately crash, meaning that it is possible for the process to remain in this state until an administrator intervenes or an automated circuit breaker fires. If left unchecked this issue will very slowly exhaust memory resources due to repeated buffer allocation, but the buffers are not written to and so it is possible that the processes will not terminate for quite some time. This risk can be mitigated by removing transparent HTTP message decompression. The issue is fixed by correctly detecting the termination of the compressed body as reported by zlib and refusing to decompress further data. The issue was found by Vojtech Rylko (https://github.com/vojtarylko) and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reported publicly on GitHub. **CVE ID : CVE-2022-3252**		
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.10.3					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Sep-2022	7.5	Improper detection of complete HTTP body decompression SwiftNIO Extras provides a pair of helpers for transparently decompressing received HTTP request or response bodies. These two objects (HTTPRequestDecompressor and HTTPResponseDecompressor) both failed to detect when the decompressed body was considered complete. If trailing junk data was appended to the HTTP message body, the code would repeatedly attempt to decompress this data and fail. This would lead to an infinite loop making no forward progress, leading to livelock of the system and denial-of-service. This	N/A	A-APP-SWIF-101022/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue can be triggered by any attacker capable of sending a compressed HTTP message. Most commonly this is HTTP servers, as compressed HTTP messages cannot be negotiated for HTTP requests, but it is possible that users have configured decompression for HTTP requests as well. The attack is low effort, and likely to be reached without requiring any privilege or system access. The impact on availability is high: the process immediately becomes unavailable but does not immediately crash, meaning that it is possible for the process to remain in this state until an administrator intervenes or an automated circuit breaker fires. If left unchecked this issue will very slowly exhaust memory resources due to repeated		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer allocation, but the buffers are not written to and so it is possible that the processes will not terminate for quite some time. This risk can be mitigated by removing transparent HTTP message decompression. The issue is fixed by correctly detecting the termination of the compressed body as reported by zlib and refusing to decompress further data. The issue was found by Vojtech Rylko (https://github.com/vojtarylko) and reported publicly on GitHub. **CVE ID : CVE-2022-3252**		
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.14.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-Sep-2022	7.5	Improper detection of complete HTTP body decompression SwiftNIO Extras provides a pair of helpers for transparently decompressing received HTTP request or response bodies.	N/A	A-APP-SWIF-101022/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These two objects (HTTPRequestDecompressor and HTTPResponseDecompressor) both failed to detect when the decompressed body was considered complete. If trailing junk data was appended to the HTTP message body, the code would repeatedly attempt to decompress this data and fail. This would lead to an infinite loop making no forward progress, leading to livelock of the system and denial-of-service. This issue can be triggered by any attacker capable of sending a compressed HTTP message. Most commonly this is HTTP servers, as compressed HTTP messages cannot be negotiated for HTTP requests, but it is possible that users have configured decompression for HTTP requests as well. The attack is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low effort, and likely to be reached without requiring any privilege or system access. The impact on availability is high: the process immediately becomes unavailable but does not immediately crash, meaning that it is possible for the process to remain in this state until an administrator intervenes or an automated circuit breaker fires. If left unchecked this issue will very slowly exhaust memory resources due to repeated buffer allocation, but the buffers are not written to and so it is possible that the processes will not terminate for quite some time. This risk can be mitigated by removing transparent HTTP message decompression. The issue is fixed by correctly detecting the termination of the compressed body		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as reported by zlib and refusing to decompress further data. The issue was found by Vojtech Rylko (https://github.com/vojtarylko) and reported publicly on GitHub. **CVE ID : CVE-2022-3252**		
Product: swiftnio					
Affected Version(s): * Up to (excluding) 2.29.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Sep-2022	7.5	NIOHTTP1 and projects using it for generating HTTP responses can be subject to a HTTP Response Injection attack. This occurs when a HTTP/1.1 server accepts user generated input from an incoming request and reflects it into a HTTP/1.1 response header in some form. A malicious user can add newlines to their input (usually in encoded form) and "inject" those newlines into the returned HTTP response. This capability allows users to work around security headers and HTTP/1.1 framing	N/A	A-APP-SWIF-101022/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			headers by injecting entirely false responses or other new headers. The injected false responses may also be treated as the response to subsequent requests, which can lead to XSS, cache poisoning, and a number of other flaws. This issue was resolved by adding validation to the HTTPHeaders type, ensuring that there's no whitespace incorrectly present in the HTTP headers provided by users. As the existing API surface is non-failable, all invalid characters are replaced by linear whitespace. **CVE ID : CVE-2022-3215**		
Affected Version(s): From (including) 2.30.0 Up to (excluding) 2.39.1					
Improper Neutralization of Special Elements in Output Used by a Downstream	28-Sep-2022	7.5	NIOHTTP1 and projects using it for generating HTTP responses can be subject to a HTTP Response Injection attack. This occurs when a HTTP/1.1 server accepts user	N/A	A-APP-SWIF-101022/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			generated input from an incoming request and reflects it into a HTTP/1.1 response header in some form. A malicious user can add newlines to their input (usually in encoded form) and "inject" those newlines into the returned HTTP response. This capability allows users to work around security headers and HTTP/1.1 framing headers by injecting entirely false responses or other new headers. The injected false responses may also be treated as the response to subsequent requests, which can lead to XSS, cache poisoning, and a number of other flaws. This issue was resolved by adding validation to the HTTPHeaders type, ensuring that there's no whitespace incorrectly present in the HTTP headers provided		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by users. As the existing API surface is non-failable, all invalid characters are replaced by linear whitespace. **CVE ID : CVE-2022-3215**		
Affected Version(s): From (including) 2.40.0 Up to (excluding) 2.42.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	28-Sep-2022	7.5	NIOHTTP1 and projects using it for generating HTTP responses can be subject to a HTTP Response Injection attack. This occurs when a HTTP/1.1 server accepts user generated input from an incoming request and reflects it into a HTTP/1.1 response header in some form. A malicious user can add newlines to their input (usually in encoded form) and "inject" those newlines into the returned HTTP response. This capability allows users to work around security headers and HTTP/1.1 framing headers by injecting entirely false responses or other new headers.	N/A	A-APP-SWIF-101022/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The injected false responses may also be treated as the response to subsequent requests, which can lead to XSS, cache poisoning, and a number of other flaws. This issue was resolved by adding validation to the HTTPHeaders type, ensuring that there's no whitespace incorrectly present in the HTTP headers provided by users. As the existing API surface is non-failable, all invalid characters are replaced by linear whitespace. **CVE ID : CVE-2022-3215**		
Vendor: Arubanetworks					
Product: clearpass_policy_manager					
Affected Version(s): From (including) 6.10.0 Up to (excluding) 6.10.7					
Cross-Site Request Forgery (CSRF)	20-Sep-2022	8.8	A vulnerability in the ClearPass Policy Manager web-based management interface exists which exposes some endpoints to a lack of Cross-Site Request Forgery	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CSRF) protection. This could allow a remote unauthenticated attacker to execute arbitrary input against these endpoints if the attacker can convince an authenticated user of the interface to interact with a specially crafted URL in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2022-23685**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-23692**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-23693**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-23694**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-23695**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-23696**		
N/A	20-Sep-2022	7.8	A vulnerability in the ClearPass OnGuard macOS agent could allow malicious users on a macOS instance to elevate their user privileges. A successful exploit could allow these users to execute arbitrary code with root level privileges on the macOS instance in Aruba ClearPass Policy Manager version(s): 6.10.x:	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2022-37877**		
N/A	20-Sep-2022	7.5	A vulnerability exists in the ClearPass Policy Manager Guest User Interface that can allow an unauthenticated attacker to send specific operations which result in a Denial-of-Service condition. A successful exploitation of this vulnerability results in the unavailability of the guest interface in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address this security vulnerability.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37884		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37878**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/194
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based	https://www.arubanetworks.com/assets/alert/	A-ARU-CLEA-101022/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37879**	ARUBA-PSA-2022-013.txt	
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37880**		
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37881**		
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37882**		
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37883**		
Affected Version(s): From (including) 6.9.0 Up to (excluding) 6.9.12					
Cross-Site Request Forgery (CSRF)	20-Sep-2022	8.8	A vulnerability in the ClearPass Policy Manager web-based management interface exists which exposes some endpoints to a lack of Cross-Site Request Forgery (CSRF) protection. This could allow a remote unauthenticated attacker to execute arbitrary input against these endpoints if the attacker can convince an authenticated user of the interface to interact with a specially crafted URL in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2022-23685**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager that address these security vulnerabilities. **CVE ID : CVE-2022-23692**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address these security vulnerabilities. **CVE ID : CVE-2022-23693**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-23694**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-23695**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-23696**		
N/A	20-Sep-2022	7.8	A vulnerability in the ClearPass OnGuard macOS agent could allow malicious users on a macOS instance to elevate their user privileges. A successful exploit could allow these users to execute arbitrary code with root level privileges on the macOS instance in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2022-37877**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/206
N/A	20-Sep-2022	7.5	A vulnerability exists in the ClearPass Policy Manager Guest User Interface that can allow an unauthenticated attacker to send specific operations	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which result in a Denial-of-Service condition. A successful exploitation of this vulnerability results in the unavailability of the guest interface in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2022-37884**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37878**		
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x:	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37879**		
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37880**		
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37881**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37882**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/212
N/A	20-Sep-2022	7.2	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	A-ARU-CLEA-101022/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address these security vulnerabilities. **CVE ID : CVE-2022-37883**		
Vendor: arvados					
Product: arvados					
Affected Version(s): * Up to (excluding) 2.4.3					
Improper Authentication	23-Sep-2022	8.8	Arvados is an open source platform for managing and analyzing biomedical big data. In versions prior to 2.4.3, when using Portable	https://github.com/arvados/arvados/security/advisories/GHSA-87jr-xwhg-cxjv	A-ARV-ARVA-101022/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authentication Modules (PAM) for user authentication, if a user presented valid credentials but the account is disabled or otherwise not allowed to access the host (such as an expired password), it would still be accepted for access to Arvados. Other authentication methods (LDAP, OpenID Connect) supported by Arvados are not affected by this flaw. This issue is patched in version 2.4.3. Workaround for this issue is to migrate to a different authentication method supported by Arvados, such as LDAP. **CVE ID : CVE-2022-39238**		
Vendor: aspiresoftware					
Product: open_aviation_strategic_engineering_system					
Affected Version(s): 8.8.0.2					
N/A	16-Sep-2022	8.8	OASES (aka Open Aviation Strategic Engineering System) 8.8.0.2 allows attackers to	https://www.aspiresoftware.com/companies/oases/	A-ASP-OPEN-101022/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code via the Open Print Folder menu. **CVE ID : CVE-2022-40337**		
Vendor: Asus					
Product: armoury_crate_service					
Affected Version(s): * Up to (excluding) 5.2.10.0					
Improper Link Resolution Before File Access ('Link Following')	28-Sep-2022	5.9	Armoury Crate Service's logging function has insufficient validation to check if the log file is a symbolic link. A physical attacker with general user privilege can modify the log file property to a symbolic link that points to arbitrary system file, causing the logging function to overwrite the system file and disrupt the system. **CVE ID : CVE-2022-38699**	N/A	A-ASU-ARMO-101022/216
Vendor: autoptimize					
Product: autoptimize					
Affected Version(s): * Up to (excluding) 3.1.1					
Improper Neutralization of Input During Web Page Generation	16-Sep-2022	4.8	The Autoptimize WordPress plugin before 3.1.1 does not sanitise and escape some of its settings, which could allow high privilege users	N/A	A-AUT-AUTO-101022/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2635**		
Vendor: awesome					
Product: torro_forms					
Affected Version(s): * Up to (including) 1.0.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Awesome UG Torro Forms plugin <= 1.0.16 at WordPress. **CVE ID : CVE-2022-36791**	https://wordpress.org/plugins/torro-forms/, https://patchstack.com/database/vulnerability/torro-forms/wordpress-torro-forms-plugin-1-0-16-authenticated-stored-cross-site-scripting-xss-vulnerability/_s_id=cve	A-AWE-TORR-101022/218
Vendor: axiosys					
Product: bento4					
Affected Version(s): * Up to (including) 1.6.0-639					
NULL Pointer Dereference	18-Sep-2022	5.5	An issue was discovered in Bento4 through 1.6.0-639. There is a NULL pointer dereference in AP4_StszAtom::GetSampleSize.	N/A	A-AXI-BENT-101022/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40774		
NULL Pointer Dereference	18-Sep-2022	5.5	An issue was discovered in Bento4 through 1.6.0-639. A NULL pointer dereference occurs in AP4_StszAtom::WriteFields. **CVE ID : CVE-2022-40775**	N/A	A-AXI-BENT-101022/220
Vendor: B2evolution					
Product: b2evolution					
Affected Version(s): * Up to (excluding) 7.2.5					
Use of Insufficiently Random Values	28-Sep-2022	9.1	An authorization bypass in b2evolution allows remote, unauthenticated attackers to predict password reset tokens for any user through the use of a bad randomness function. This allows the attacker to get valid sessions for arbitrary users, and optionally reset their password. Tested and confirmed in a default installation of version 7.2.3. Earlier versions are affected, possibly earlier major versions as well.	https://b2evolution.net/downloads/7-2-5-stable, https://github.com/b2evolution/b2evolution/blob/master/inc/_core/_misc.funcs.php#L5955	A-B2E-B2EV-101022/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30935		
Vendor: backup_scheduler_project					
Product: backup_scheduler					
Affected Version(s): * Up to (including) 1.5.13					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability Backup Scheduler plugin <= 1.5.13 at WordPress. **CVE ID : CVE-2022-38079**	https://patchstack.com/database/vulnerability/backup-scheduler/wordpress-backup-scheduler-plugin-1-5-13-cross-site-request-forgery-csrf-vulnerability/_s_id=cve, https://wordpress.org/plugins/backup-scheduler/	A-BAC-BACK-101022/222
Vendor: badgeos					
Product: badgos					
Affected Version(s): * Up to (excluding) 3.7.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	8.8	The BadgeOS WordPress plugin before 3.7.1.3 does not sanitise and escape parameters before using them in SQL statements via AJAX actions available to any authenticated users, leading to SQL Injections **CVE ID : CVE-2022-2958**	https://wpscan.com/vulnerability/8743534f-8ebd-496a-99bc-5052a8bac86a	A-BAD-BADG-101022/223
Vendor: baijiacms_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: baijiacms					
Affected Version(s): 4.1.4					
Server-Side Request Forgery (SSRF)	20-Sep-2022	8.8	A Server-Side Request Forgery (SSRF) in fetch_net_file_upload function of baijiacmsV4 v4.1.4 allows remote attackers to force the application to make arbitrary requests via injection of arbitrary URLs into the url parameter. **CVE ID : CVE-2022-38931**	N/A	A-BAI-BAIJ-101022/224
Vendor: basixonline					
Product: nex-forms					
Affected Version(s): * Up to (excluding) 7.9.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	8.8	The NEX-Forms WordPress plugin before 7.9.7 does not properly sanitise and escape user input before using it in SQL statements, leading to SQL injections. The attack can be executed by anyone who is permitted to view the forms statistics chart, by default administrators, however can be configured otherwise via the plugin settings.	N/A	A-BAS-NEX--101022/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3142		
Vendor: bigfile					
Product: bigfileagent					
Affected Version(s): * Up to (excluding) 1.0.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	8.8	An improper input validation vulnerability leading to arbitrary file execution was discovered in BigFileAgent. In order to cause arbitrary files to be executed, the attacker makes the victim access a web page d by them or inserts a script using XSS into a general website. **CVE ID : CVE-2022-23766**	N/A	A-BIG-BIGF-101022/226
Vendor: bitcoin\/altcoin_faucet_project					
Product: bitcoin\/altcoin_faucet					
Affected Version(s): * Up to (including) 1.6.0					
Cross-Site Request Forgery (CSRF)	26-Sep-2022	5.4	The Bitcoin / Altcoin Faucet WordPress plugin through 1.6.0 does not have any CSRF check when saving its settings, allowing attacker to make a logged in admin change them via a CSRF attack. Furthermore, due to the lack of sanitisation and escaping, it could	N/A	A-BIT-BITC-101022/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also lead to Stored Cross-Site Scripting issues **CVE ID : CVE-2022-3025**		
Vendor: blazzdev					
Product: rate_my_post_-_wp_rating_system					
Affected Version(s): * Up to (including) 3.3.4					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Rate my Post – WP Rating System plugin <= 3.3.4 at WordPress. **CVE ID : CVE-2022-40671**	https://patchstack.com/database/vulnerability/rate-my-post/wordpress-rate-my-post-wp-rating-system-plugin-3-3-4-cross-site-request-forgery-csrf-vulnerability/_s_id=cve, https://wordpress.org/plugins/rate-my-post/#developers	A-BLA-RATE-101022/228
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	23-Sep-2022	3.1	Authenticated (subscriber+) Race Condition vulnerability in Rate my Post – WP Rating System plugin <= 3.3.4 at WordPress allows attackers to increase/decrease votes. **CVE ID : CVE-2022-40310**	https://patchstack.com/database/vulnerability/rate-my-post/wordpress-rate-my-post-wp-rating-system-plugin-3-3-4-race-condition-vulnerability/_s_id=cve, https://wordpress.org/plugins/rate-my-	A-BLA-RATE-101022/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				post/#developers	
Vendor: blossomthemes					
Product: blossom_recipe_maker					
Affected Version(s): * Up to (including) 1.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in Blossom Recipe Maker plugin <= 1.0.7 at WordPress. **CVE ID : CVE-2022-37338**	https://wordpress.org/plugins/blossom-recipe-maker/, https://patchstack.com/database/vulnerability/blossom-recipe-maker/wordpress-blossom-recipe-maker-plugin-1-0-7-multiple-authenticated-stored-cross-site-scripting-xss-vulnerabilities	A-BLO-BLOS-101022/230
Vendor: Bolt					
Product: bolt_cms					
Affected Version(s): * Up to (including) 5.1.12					
N/A	16-Sep-2022	8.8	Bolt CMS contains a vulnerability in version 5.1.12 and below that allows an authenticated user with the ROLE_EDITOR privileges to upload and rename a malicious file to achieve remote code execution. **CVE ID : CVE-2022-36532**	N/A	A-BOL-BOLT-101022/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: bpcbt					
Product: smartvista					
Affected Version(s): 2.2.22					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	8.8	SmartVista SVFE2 v2.2.22 was discovered to contain a SQL injection vulnerability via the voiceAudit:j_id97 parameter at /SVFE2/pages/audit/voiceaudit.jsf. **CVE ID : CVE-2022-38617**	N/A	A-BPC-SMAR-101022/232
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	8.8	SmartVista SVFE2 v2.2.22 was discovered to contain a SQL injection vulnerability via the UserForm:j_id88, UserForm:j_id90, and UserForm:j_id92 parameters at /SVFE2/pages/feegroups/country_group.jsf. **CVE ID : CVE-2022-38618**	N/A	A-BPC-SMAR-101022/233
Product: smartvista_front-end					
Affected Version(s): 2.2.22					
Improper Neutralization of Special Elements used in an	21-Sep-2022	9.8	SmartVista SVFE2 v2.2.22 was discovered to contain a SQL injection vulnerability via	http://bpcbt.com	A-BPC-SMAR-101022/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			the UserForm:j_id90 parameter at /SVFE2/pages/feegroups/mcc_group.jsf. **CVE ID : CVE-2022-38619**		
Vendor: brinidesigner					
Product: awesome_filterable_portfolio					
Affected Version(s): * Up to (including) 1.9.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability in Awesome Filterable Portfolio plugin <= 1.9.7 at WordPress. **CVE ID : CVE-2022-40193**	https://wordpress.org/plugins/awesome-filterable-portfolio/	A-BRI-AWES-101022/235
N/A	23-Sep-2022	5.3	Unauthenticated Plugin Settings Change vulnerability in Awesome Filterable Portfolio plugin <= 1.9.7 at WordPress. **CVE ID : CVE-2022-35238**	https://wordpress.org/plugins/awesome-filterable-portfolio/, https://patchstack.com/database/vulnerability/awesome-filterable-portfolio/wordpress-awesome-filterable-portfolio-plugin-1-9-7-unauthenticated-plugin-settings-change-	A-BRI-AWES-101022/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				vulnerability/_s_id=cve	
Vendor: budibase					
Product: budibase					
Affected Version(s): * Up to (excluding) 1.3.20					
Improper Access Control	16-Sep-2022	5.7	Improper Access Control in GitHub repository budibase/budibase prior to 1.3.20. **CVE ID : CVE-2022-3225**	https://github.com/budibase/budibase/commit/d35864be0854216693a01307f81ffcabf6d549df, https://huntr.dev/bounties/a13a56b7-04da-4560-b8ec-0d637d12a245	A-BUD-BUDI-101022/237
Vendor: cagewebdesign					
Product: float_to_top_button					
Affected Version(s): * Up to (including) 2.3.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	4.8	The Float to Top Button WordPress plugin through 2.3.6 does not escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2709**	N/A	A-CAG-FLOA-101022/238
Vendor: castos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: seriously_simple_podcasting					
Affected Version(s): * Up to (including) 2.16.0					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Seriously Simple Podcasting plugin <= 2.16.0 at WordPress, leading to plugin settings change. **CVE ID : CVE-2022-40132**	https://patchstack.com/database/vulnerability/seriously-simple-podcasting/wordpress-seriously-simple-podcasting-plugin-2-16-0-cross-site-request-forgery-csrf-vulnerability/_s_id=cve, https://wordpress.org/plugins/seriously-simple-podcasting/#developers	A-CAS-SERI-101022/239
Vendor: Centreon					
Product: centreon					
Affected Version(s): 20.10.18					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	8.8	Centreon v20.10.18 was discovered to contain a SQL injection vulnerability via the esc_name (Escalation Name) parameter at Configuration/Notifications/Escalations. **CVE ID : CVE-2022-40043**	N/A	A-CEN-CENT-101022/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	5.4	Centreon v20.10.18 was discovered to contain a cross-site scripting (XSS) vulnerability via the esc_name (Escalation Name) parameter at Configuration/Notifications/Escalations. This vulnerability allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload. **CVE ID : CVE-2022-40044**	N/A	A-CEN-CENT-101022/241
Vendor: Checkpoint					
Product: zonealarm					
Affected Version(s): * Up to (excluding) 15.8.211.19229					
Improper Privilege Management	27-Sep-2022	8.8	Check Point ZoneAlarm Extreme Security before 15.8.211.19229 allows local users to escalate privileges. This occurs because of weak permissions for the %PROGRAMDATA%\CheckPoint\ZoneAlarm\Data\Updates directory, and a self-protection driver bypass that allows creation of a junction directory.	https://www.zonealarm.com/software/extreme-security/release-history	A-CHE-ZONE-101022/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This can be leveraged to perform an arbitrary file move as NT AUTHORITY\SYSTEM. **CVE ID : CVE-2022-41604**		
Vendor: clogica					
Product: seo_redirection					
Affected Version(s): * Up to (including) 8.9					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in SEO Redirection plugin <= 8.9 at WordPress, leading to deletion of 404 errors and redirection history. **CVE ID : CVE-2022-38704**	https://wordpress.org/plugins/seo-redirection/#developers, https://patchstack.com/database/vulnerability/seo-redirection/wordpress-seo-redirection-plugin-8-9-cross-site-request-forgery-csrf-vulnerability/_s_id=cve	A-CLO-SEO_-101022/243
Vendor: cloudbase					
Product: open_vswitch					
Affected Version(s): From (including) 0.90.0 Up to (including) 2.5.0					
Out-of-bounds Read	28-Sep-2022	8.8	In ovs versions v0.90.0 through v2.5.0 are vulnerable to heap buffer over-read in flow.c. An unsafe comparison of “minimasks”	https://github.com/cloudbase/ovs/commit/2ed6505555cdcb46f9b1f0329d1491b75290fc73	A-CLO-OPEN-101022/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function could lead access to an unmapped region of memory. This vulnerability is capable of crashing the software, memory modification, and possible remote execution. **CVE ID : CVE-2022-32166**		
Vendor: cloudreve					
Product: cloudreve					
Affected Version(s): From (including) 1.0.0 Up to (including) 3.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	5.4	Cloudreve versions v1.0.0 through v3.5.3 are vulnerable to Stored Cross-Site Scripting (XSS), via the file upload functionality. A low privileged user will be able to share a file with an admin user, which could lead to privilege escalation. **CVE ID : CVE-2022-32167**	N/A	A-CLO-CLOU-101022/245
Vendor: cloudwego					
Product: hertz					
Affected Version(s): 0.3.0					
Improper Limitation of a Pathname to a Restricted	28-Sep-2022	7.5	Hertz v0.3.0 ws discovered to contain a path traversal vulnerability via	https://github.com/cloudwego/hertz/pull/229	A-CLO-HERT-101022/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			the normalizePath function. **CVE ID : CVE-2022-40082**		
Vendor: cm-wp					
Product: titan_anti-spam_\&_security					
Affected Version(s): * Up to (excluding) 7.3.1					
Authorization Bypass Through User-Controlled Key	16-Sep-2022	5.3	The Titan Anti-spam & Security WordPress plugin before 7.3.1 does not properly checks HTTP headers in order to validate the origin IP address, allowing threat actors to bypass it's block feature by spoofing the headers. **CVE ID : CVE-2022-2877**	N/A	A-CM--TITA-101022/247
Vendor: Cminds					
Product: cm_download_manager					
Affected Version(s): * Up to (excluding) 2.8.6					
Unrestricted Upload of File with Dangerous Type	26-Sep-2022	7.2	The CM Download Manager WordPress plugin before 2.8.6 allows high privilege users such as admin to upload arbitrary files by setting the any extension via the plugin's setting, which could be used by admins of multisite blog to	https://wpscan.com/vulnerability/d18e695b-4d6e-4ff6-a060-312594a0d2bd	A-CMI-CM_D-101022/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload PHP files for example. **CVE ID : CVE-2022-3076**		
Vendor: Codepeople					
Product: form_builder_cp					
Affected Version(s): * Up to (excluding) 1.2.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	4.8	The Form Builder CP WordPress plugin before 1.2.32 does not sanitise and escape some of its form settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2567**	https://wpscan.com/vulnerability/dfa21dde-a9fc-4a35-9602-c3fde907ca54	A-COD-FORM-101022/249
Vendor: connectwise					
Product: connectwise					
Affected Version(s): * Up to (excluding) 22.7					
Improper Restriction of Excessive Authentication Attempts	28-Sep-2022	5.3	WiseConnect - ScreenConnect Session Code Bypass. An attacker would have to use a proxy to monitor the traffic, and perform a brute force on the session code in order to get in.	N/A	A-CON-CONN-101022/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sensitive data about the company , get in a session. **CVE ID : CVE-2022-36781**		
Vendor: cowell_enterprise_travel_management_system_project					
Product: cowell_enterprise_travel_management_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	6.1	Cowell enterprise travel management system has insufficient filtering for special characters within web URL. An unauthenticated remote attacker can inject JavaScript and perform XSS (Reflected Cross-Site Scripting) attack. **CVE ID : CVE-2022-39054**	N/A	A-COW-COWE-101022/251
Vendor: cozmoslabs					
Product: translatepress					
Affected Version(s): * Up to (excluding) 2.3.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	8.8	The Translate Multilingual sites WordPress plugin before 2.3.3 is vulnerable to an authenticated SQL injection. By adding a new language (via the settings page) containing specific special characters, the backticks in the	N/A	A-COZ-TRAN-101022/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SQL query can be surpassed and a time-based blind payload can be injected. **CVE ID : CVE-2022-3141**		
Vendor: Craftcms					
Product: craft_cms					
Affected Version(s): 4.2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Craft CMS 4.2.0.1 is affected by Cross Site Scripting (XSS) in the file src/web/assets/cp/src/js/BaseElementSelectInput.js and in specific on the line label: elementInfo.label. **CVE ID : CVE-2022-37246**	https://github.com/craftcms/cms/commit/1d5fdba23c84d6d09a8a980c7b6fc52fb93b679b, https://labs.integrity.pt/advisories/cve-2022-37246/	A-CRA-CRAF-101022/253
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Craft CMS 4.2.0.1 is vulnerable to stored a cross-site scripting (XSS) via /admin/settings/fields page. **CVE ID : CVE-2022-37247**	https://github.com/craftcms/cms/commit/cedeba0609e4b173cd584dae7f33c5f713f19627	A-CRA-CRAF-101022/254
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Craft CMS 4.2.0.1 is vulnerable to Cross Site Scripting (XSS) via src/helpers/Cp.php. **CVE ID : CVE-2022-37248**	https://github.com/craftcms/cms/commit/cedeba0609e4b173cd584dae7f33c5f713f19627, https://labs.integrity.pt/advisories/cve-2022-37248/	A-CRA-CRAF-101022/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Craft CMS 4.2.0.1 suffers from Stored Cross Site Scripting (XSS) in /admin/myaccount. **CVE ID : CVE-2022-37250**	https://labs.integrity.pt/advisories/cve-2022-37250/, https://github.com/craftcms/cms/commit/cdc9cb66d0716c9552e4113c8e426fd1a31f9516	A-CRA-CRAF-101022/256
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Craft CMS 4.2.0.1 is vulnerable to Cross Site Scripting (XSS) via Drafts. **CVE ID : CVE-2022-37251**	N/A	A-CRA-CRAF-101022/257
Vendor: craw-data_project					
Product: craw-data					
Affected Version(s): * Up to (including) 1.0.0					
Server-Side Request Forgery (SSRF)	16-Sep-2022	4.3	The Craw Data WordPress plugin through 1.0.0 does not implement nonce checks, which could allow attackers to make a logged in admin change the url value performing unwanted crawls on third-party sites (SSRF). **CVE ID : CVE-2022-2912**	N/A	A-CRA-CRAW-101022/258
Vendor: creativeitem					
Product: academy_learning_management_system					
Affected Version(s): * Up to (excluding) 5.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	6.1	Academy Learning Management System before v5.9.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the Search parameter. **CVE ID : CVE-2022-38553**	N/A	A-CRE-ACAD-101022/259
Vendor: Crestron					
Product: airmedia					
Affected Version(s): 4.3.1.39					
N/A	23-Sep-2022	8.8	Crestron AirMedia for Windows before 5.5.1.84 has insecure inherited permissions, which leads to a privilege escalation vulnerability found in the AirMedia Windows Application, version 4.3.1.39. A low privileged user can initiate a repair of the system and gain a SYSTEM level shell. **CVE ID : CVE-2022-40298**	https://www.crestron.com/Security/Security_Advisories, https://www.crestron.com/release_notes/airmedia_windows_installer_release_notes_5.5.1.84.pdf	A-CRE-AIRM-101022/260
Vendor: cusrev					
Product: customer_reviews_for_woocommerce					
Affected Version(s): * Up to (including) 5.3.5					
N/A	23-Sep-2022	8.8	Authenticated (subscriber+) Broken Access Control	https://wordpress.org/plugins/customer-reviews-	A-CUS-CUST-101022/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in Customer Reviews for WooCommerce plugin <= 5.3.5 at WordPress. **CVE ID : CVE-2022-38134**	woocommerce/#developers	
Cross-Site Request Forgery (CSRF)	23-Sep-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Customer Reviews for WooCommerce plugin <= 5.3.5 at WordPress. **CVE ID : CVE-2022-38470**	https://wordpress.org/plugins/customer-reviews-woocommerce/#developers	A-CUS-CUST-101022/262
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-2022	7.5	Unauthenticated Sensitive Information Disclosure vulnerability in Customer Reviews for WooCommerce plugin <= 5.3.5 at WordPress **CVE ID : CVE-2022-40194**	https://patchstack.com/database/vulnerability/customer-reviews-woocommerce/wordpress-customer-reviews-for-woocommerce-plugin-5-3-5-sensitive-information-disclosure-vulnerability/_s_id=cve	A-CUS-CUST-101022/263
Vendor: d8s-archives_project					
Product: d8s-archives					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-archives for python, as distributed on PyPI, included a potential code-execution	N/A	A-D8S-D8S--101022/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backdoor inserted by a third party. The backdoor is the democritus-strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38881**		
Vendor: d8s-asns_project					
Product: d8s-asns					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-asns for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The affected version is 0.1.0. **CVE ID : CVE-2022-40426**	N/A	A-D8S-D8S--101022/265
Vendor: d8s-grammars_project					
Product: d8s-grammars					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-grammars for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-	N/A	A-D8S-D8S--101022/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38884**		
Vendor: d8s-html_project					
Product: d8s-html					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-html for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The affected version is 0.1.0. **CVE ID : CVE-2022-40425**	N/A	A-D8S-D8S--101022/267
Vendor: d8s-ip-addresses_project					
Product: d8s-ip-addresses					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-ip-addresses for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The	N/A	A-D8S-D8S--101022/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected version is 0.1.0. **CVE ID : CVE-2022-40429**		
Vendor: d8s-json_project					
Product: d8s-json					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-json for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38882**	N/A	A-D8S-D8S--101022/269
Vendor: d8s-math_project					
Product: d8s-math					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-math for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38883**	N/A	A-D8S-D8S--101022/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: d8s-mpeg_project					
Product: d8s_mpeg					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-mpeg for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The affected version is 0.1.0. **CVE ID : CVE-2022-40428**	N/A	A-D8S-D8S_-101022/271
Vendor: d8s-netstrings_project					
Product: d8s-netstrings					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-netstrings for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38885**	N/A	A-D8S-D8S--101022/272
Vendor: d8s-pdfs_project					
Product: d8s-pdfs					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-pdfs for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The affected version is 0.1.0. **CVE ID : CVE-2022-40431**	N/A	A-D8S-D8S--101022/273
Vendor: d8s-python_project					
Product: d8s-python					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-python for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The democritus-strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38887**	N/A	A-D8S-D8S--101022/274
Vendor: d8s-strings_project					
Product: d8s-strings					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with	19-Sep-2022	9.8	The d8s-strings for python, as distributed on	N/A	A-D8S-D8S--101022/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hypothesis package. The affected version is 0.1.0. **CVE ID : CVE-2022-40432**		
Vendor: d8s-utility_project					
Product: d8s-utility					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-utility for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The affected version is 0.1.0. **CVE ID : CVE-2022-40430**	N/A	A-D8S-D8S--101022/276
Vendor: d8s-xml_project					
Product: d8s-xml					
Affected Version(s): 0.1.0					
Unrestricted Upload of File with Dangerous Type	19-Sep-2022	9.8	The d8s-xml for python, as distributed on PyPI, included a potential code-execution	N/A	A-D8S-D8S--101022/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backdoor inserted by a third party. The backdoor is the democritus-strings package. The affected version is 0.1.0. **CVE ID : CVE-2022-38886**		
Vendor: databank					
Product: accreditation_tracking\/presentation_module					
Affected Version(s): * Up to (excluding) 2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Sep-2022	9.8	Database Software Accreditation Tracking/Presentation Module product before version 2 has an unauthenticated SQL Injection vulnerability. This is fixed in version 2. **CVE ID : CVE-2022-2315**	https://www.usom.gov.tr/bildirim/tr-22-0634	A-DAT-ACCR-101022/278
Vendor: deltaww					
Product: diaenergie					
Affected Version(s): * Up to (excluding) 1.9.0					
Use of Hard-coded Credentials	16-Sep-2022	9.8	Delta Industrial Automation's DIAEnergy, an industrial energy management system, is vulnerable to CWE-798, Use of Hard-coded Credentials. Version 1.8.0 and prior have this vulnerability. Executable files	N/A	A-DEL-DIAE-101022/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be uploaded to certain directories using hard-coded bearer authorization, allowing remote code execution. **CVE ID : CVE-2022-3214**		
Vendor: democritus_dates_project					
Product: democritus_dates					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-dates for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hypothesis package. The affected version is 0.1.0 **CVE ID : CVE-2022-40808**	N/A	A-DEM-DEMO-101022/280
Vendor: democritus_dicts_project					
Product: democritus_dicts					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-dicts for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-	N/A	A-DEM-DEMO-101022/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hypothesis package. The affected version is 0.1.0 **CVE ID : CVE-2022-40809**		
Vendor: democritus_domains_project					
Product: democritus_domains					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-domains for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-networking package. The affected version is 0.1.0 **CVE ID : CVE-2022-40427**	N/A	A-DEM-DEMO-101022/282
N/A	19-Sep-2022	9.8	The d8s-domains for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hypothesis package. The affected version is 0.1.0 **CVE ID : CVE-2022-40807**	N/A	A-DEM-DEMO-101022/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: democritus_ip_addresses_project					
Product: democritus_ip_addresses					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-ip-addresses for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hypothesis package. The affected version is 0.1.0 **CVE ID : CVE-2022-40810**	N/A	A-DEM-DEMO-101022/284
Vendor: democritus_pdfs_project					
Product: democritus_pdfs					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-pdfs for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-file-system package. The affected version is 0.1.0. **CVE ID : CVE-2022-40812**	N/A	A-DEM-DEMO-101022/285
Vendor: democritus_urls_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: democritus_urls					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-urls for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The affected version is 0.1.0. **CVE ID : CVE-2022-38880**	N/A	A-DEM-DEMO-101022/286
N/A	19-Sep-2022	9.8	The d8s-urls for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code execution backdoor inserted by third parties is the democritus-networking package. The affected version of d8s-urls is 0.1.0 **CVE ID : CVE-2022-40424**	N/A	A-DEM-DEMO-101022/287
N/A	19-Sep-2022	9.8	The d8s-urls for python 0.1.0, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. A potential code	N/A	A-DEM-DEMO-101022/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution backdoor inserted by third parties is the democritus-hypothesis package. **CVE ID : CVE-2022-40805**		
N/A	19-Sep-2022	9.8	The d8s-urls for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-file-system package. The affected version is 0.1.0. **CVE ID : CVE-2022-40811**	N/A	A-DEM-DEMO-101022/289
Vendor: democritus_uuids_project					
Product: democritus_uuids					
Affected Version(s): 0.1.0					
N/A	19-Sep-2022	9.8	The d8s-uuids for python, as distributed on PyPI, included a potential code-execution backdoor inserted by a third party. The backdoor is the democritus-hypothesis package. The affected version is 0.1.0	N/A	A-DEM-DEMO-101022/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40806		
Vendor: denx					
Product: u-boot					
Affected Version(s): From (including) 2012.10 Up to (including) 2022.07					
Out-of-bounds Write	23-Sep-2022	7.1	There exists an unchecked length field in UBoot. The U-Boot DFU implementation does not bound the length field in USB DFU download setup packets, and it does not verify that the transfer direction corresponds to the specified command. Consequently, if a physical attacker crafts a USB DFU download setup packet with a `wLength` greater than 4096 bytes, they can write beyond the heap-allocated request buffer. **CVE ID : CVE-2022-2347**	N/A	A-DEN-U-BO-101022/291
Vendor: diagrams					
Product: drawio					
Affected Version(s): * Up to (excluding) 20.3.1					
Improper Neutralization of Input During	16-Sep-2022	6.1	Cross-site Scripting (XSS) - Stored in GitHub repository jgraph/drawio prior to 20.3.1.	https://github.com/jgraph/drawio/commit/ea012baba6fb2e903797fa630683	A-DIA-DRAW-101022/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2022-3223**	3ca4f31ab361, https://huntr.dev/bounties/125791b6-3a68-4235-8866-6bc3a52332ba	
Vendor: diywebmastery					
Product: slickr_flickr					
Affected Version(s): * Up to (including) 2.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	4.8	The Slickr Flickr WordPress plugin through 2.8.1 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-3021**	N/A	A-DIY-SLIC-101022/293
Vendor: dompdf_project					
Product: dompdf					
Affected Version(s): * Up to (excluding) 2.0.1					
Files or Directories Accessible to External Parties	25-Sep-2022	7.5	registerFont in FontMetrics.php in Dompdf before 2.0.1 allows remote file inclusion because a URI validation failure does not halt font registration, as demonstrated by a @font-face rule.	https://github.com/dompdf/dompdf/issues/2994, https://github.com/dompdf/dompdf/pull/2995	A-DOM-DOMP-101022/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41343		
Vendor: doufox					
Product: doufox					
Affected Version(s): 0.0.4					
N/A	16-Sep-2022	9.8	Doufox v0.0.4 was discovered to contain a remote code execution (RCE) vulnerability via the edit file page. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-38621**	N/A	A-DOU-DOUF-101022/295
Vendor: Drupal					
Product: drupal					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 9.3.22					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	7.5	Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when	https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b, https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33, https://www.drupal.org/sa-core-2022-016	A-DRU-DRUP-101022/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a namespace like `@somewhere/../some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading. **CVE ID : CVE-2022-39261**		
Affected Version(s): From (including) 9.4.0 Up to (excluding) 9.4.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	7.5	Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/../some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and	https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b, https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33, https://www.drupal.org/sa-core-2022-016	A-DRU-DRUP-101022/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading. **CVE ID : CVE-2022-39261**		
Vendor: easycorp					
Product: zentao					
Affected Version(s): 15.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Sep-2022	7.5	Zentao Demo15 is vulnerable to Directory Traversal. The impact is: obtain sensitive information (remote). The component is: URL : view-source:https://demo15.zentao.pm/user-login.html/zentao/index.php?mode=getconfig. **CVE ID : CVE-2022-37700**	N/A	A-EAS-ZENT-101022/298
Vendor: Ec-cube					
Product: ec-cube					
Affected Version(s): 3.0.18					
Improper Limitation of a Pathname to a Restricted Directory	27-Sep-2022	2.7	Directory traversal vulnerability in EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p4) and EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.1.2) allows a	https://www.ec-cube.net/info/weakness/20220909/	A-EC--EC-C-101022/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			remote authenticated attacker with an administrative privilege to obtain the product's directory structure information. **CVE ID : CVE-2022-40199**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.18					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-2022	2.7	Directory traversal vulnerability in EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p4) and EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.1.2) allows a remote authenticated attacker with an administrative privilege to obtain the product's directory structure information. **CVE ID : CVE-2022-40199**	https://www.ec-cube.net/info/weakness/20220909/	A-EC--EC-C-101022/300
Affected Version(s): From (including) 4.0.0 Up to (including) 4.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-2022	5.4	DOM-based cross-site scripting vulnerability in EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.1.2) allows a remote attacker to inject an arbitrary script by having an administrative user of the product to	https://www.ec-cube.net/info/weakness/20220909/	A-EC--EC-C-101022/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visit a specially crafted page. **CVE ID : CVE-2022-38975**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Sep-2022	2.7	Directory traversal vulnerability in EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p4) and EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.1.2) allows a remote authenticated attacker with an administrative privilege to obtain the product's directory structure information. **CVE ID : CVE-2022-40199**	https://www.ec-cube.net/info/weakness/20220909/	A-EC--EC-C-101022/302
Product: product_image_bulk_upload					
Affected Version(s): 1.0.0					
Unrestricted Upload of File with Dangerous Type	27-Sep-2022	9.8	EC-CUBE plugin 'Product Image Bulk Upload Plugin' 1.0.0 and 4.1.0 contains an insufficient verification vulnerability when uploading files. Exploiting this vulnerability allows a remote unauthenticated attacker to upload arbitrary files other than image files. If a user with an administrative	https://www.ec-cube.net/info/weakness/20220909/product_images_uploader.php	A-EC--PROD-101022/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege of EC-CUBE where the vulnerable plugin is installed is led to upload a specially crafted file, an arbitrary script may be executed on the system. **CVE ID : CVE-2022-37346**		
Affected Version(s): 4.1.0					
Unrestricted Upload of File with Dangerous Type	27-Sep-2022	9.8	EC-CUBE plugin 'Product Image Bulk Upload Plugin' 1.0.0 and 4.1.0 contains an insufficient verification vulnerability when uploading files. Exploiting this vulnerability allows a remote unauthenticated attacker to upload arbitrary files other than image files. If a user with an administrative privilege of EC-CUBE where the vulnerable plugin is installed is led to upload a specially crafted file, an arbitrary script may be executed on the system. **CVE ID : CVE-2022-37346**	https://www.ec-cube.net/info/weakness/20220909/product_images_uploader.php	A-EC--PROD-101022/304
Vendor: Elastic					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: elastic_cloud_enterprise					
Affected Version(s): * Up to (excluding) 3.1.1					
Insertion of Sensitive Information into Log File	28-Sep-2022	5.3	A flaw was discovered in ECE before 3.1.1 that could lead to the disclosure of the SAML signing private key used for the RBAC features, in deployment logs in the Logging and Monitoring cluster. **CVE ID : CVE-2022-23716**	https://discuss.elastic.co/t/elastic-cloud-enterprise-3-1-1-security-update/315317	A-ELA-ELAS-101022/305
Vendor: Erlang					
Product: erlang\/otp					
Affected Version(s): * Up to (excluding) 23.3.4.15					
Improper Authentication	21-Sep-2022	9.8	In Erlang/OTP before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2, there is a Client Authentication Bypass in certain client-certification situations for SSL, TLS, and DTLS. **CVE ID : CVE-2022-37026**	https://github.com/erlang/otp/compare/OTP-23.3.4.14...OTP-23.3.4.15, https://erlangforums.com/c/erlang-news-announcements/91, https://erlangforums.com/t/otp-25-1-released/1854	A-ERL-ERLA-101022/306
Affected Version(s): From (including) 24.0 Up to (excluding) 24.3.4.2					
Improper Authentication	21-Sep-2022	9.8	In Erlang/OTP before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2, there is a Client Authentication	https://github.com/erlang/otp/compare/OTP-23.3.4.14...OTP-23.3.4.15, https://erlangforums.com/c/erl	A-ERL-ERLA-101022/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bypass in certain client-certification situations for SSL, TLS, and DTLS. **CVE ID : CVE-2022-37026**	ang-news-announcements/91, https://erlangforums.com/t/otp-25-1-released/1854	
Affected Version(s): From (including) 25.0 Up to (excluding) 25.0.2					
Improper Authentication	21-Sep-2022	9.8	In Erlang/OTP before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2, there is a Client Authentication Bypass in certain client-certification situations for SSL, TLS, and DTLS. **CVE ID : CVE-2022-37026**	https://github.com/erlang/otp/compare/OTP-23.3.4.14...OTP-23.3.4.15, https://erlangforums.com/c/erlang-news-announcements/91, https://erlangforums.com/t/otp-25-1-released/1854	A-ERL-ERLA-101022/308
Vendor: Espocrm					
Product: espocrm					
Affected Version(s): 7.1.8					
Unrestricted Upload of File with Dangerous Type	16-Sep-2022	8.8	EspoCRM version 7.1.8 is vulnerable to Unrestricted File Upload allowing attackers to upload malicious file with any extension to the server. Attacker may execute these malicious files to run unintended code on the server to compromise the server.	N/A	A-ESP-ESPO-101022/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38843		
Improper Neutralization of Formula Elements in a CSV File	16-Sep-2022	8	CSV Injection in Create Contacts in EspoCRM 7.1.8 allows remote authenticated users to run system commands via creating contacts with payloads capable of executing system commands. Admin user exporting contacts in CSV file may end up executing the malicious system commands on his system. **CVE ID : CVE-2022-38844**	N/A	A-ESP-ESPO-101022/310
Improper Neutralization of Formula Elements in a CSV File	16-Sep-2022	6.1	Cross Site Scripting in Import feature in EspoCRM 7.1.8 allows remote users to run malicious JavaScript in victim s browser via sending crafted csv file containing malicious JavaScript to authenticated user. Any authenticated user importing the crafted CSV file may end up running the malicious	N/A	A-ESP-ESPO-101022/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScripting in the browser. **CVE ID : CVE-2022-38845**		
Cleartext Transmission of Sensitive Information	16-Sep-2022	5.9	EspoCRM version 7.1.8 is vulnerable to Missing Secure Flag allowing the browser to send plain text cookies over an insecure channel (HTTP). An attacker may capture the cookie from the insecure channel using MITM attack. **CVE ID : CVE-2022-38846**	N/A	A-ESP-ESPO-101022/312
Vendor: etaplighting					
Product: etap_safety_manager					
Affected Version(s): 1.0.0.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	6.1	ETAP Lighting International NV ETAP Safety Manager 1.0.0.32 is vulnerable to Cross Site Scripting (XSS). Input passed to the GET parameter 'action' is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML/JS code in a user's browser session in context of an affected site.	N/A	A-ETA-ETAP-101022/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40912		
Vendor: evohclaimable_project					
Product: evohclaimable					
Affected Version(s): -					
N/A	21-Sep-2022	5.3	Access control vulnerability in Evoh NFT EvohClaimable contract with sha256 hash code fa2084d5abca91a62ed1d2f1cad3ec318e6a9a2d7f1510a00d898737b05f48ae allows remote attackers to execute fraudulent NFT transfers. **CVE ID : CVE-2022-35621**	N/A	A-EVO-EVOH-101022/314
Vendor: exam_reviewer_management_system_project					
Product: exam_reviewer_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-2022	9.8	Exam Reviewer Management System 1.0 is vulnerable to SQL Injection via the 'id' parameter. **CVE ID : CVE-2022-40877**	N/A	A-EXA-EXAM-101022/315
Unrestricted Upload of File with Dangerous Type	27-Sep-2022	8.8	In Exam Reviewer Management System 1.0, an authenticated attacker can upload a web-shell	N/A	A-EXA-EXAM-101022/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			php file in profile page to achieve Remote Code Execution (RCE). **CVE ID : CVE-2022-40878**		
Vendor: express_xss_sanitizer_project					
Product: express_xss_sanitizer					
Affected Version(s): * Up to (excluding) 1.1.3					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	26-Sep-2022	6.1	The package express-xss-sanitizer before 1.1.3 are vulnerable to Prototype Pollution via the allowedTags attribute, allowing the attacker to bypass xss sanitization. **CVE ID : CVE-2022-21169**	https://github.com/AhmedAdelFahim/express-xss-sanitizer/commit/3bf8aaaf4dbb1c209dcb8d87a82711a54c1ab39a, https://github.com/AhmedAdelFahim/express-xss-sanitizer/issues/4, https://security.snyk.io/vuln/SNYK-JS-EXPRESSXSSSANITIZER-3027443	A-EXP-EXPR-101022/317
Vendor: Eyesofnetwork					
Product: eyesofnetwork					
Affected Version(s): * Up to (including) 5.3-11					
Improper Neutralization of Special Elements used in an SQL Command	27-Sep-2022	9.8	An issue was discovered in EyesOfNetwork (EON) through 5.3.11. Unauthenticated SQL injection can occur.	N/A	A-EYE-EYES-101022/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-41570**		
N/A	27-Sep-2022	9.8	An issue was discovered in EyesOfNetwork (EON) through 5.3.11. Local file inclusion can occur. **CVE ID : CVE-2022-41571**	N/A	A-EYE-EYES-101022/319
Vendor: F-secure					
Product: cloud_protection_for_salesforce					
Affected Version(s): *					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Sep-2022	5.5	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.so/aerdl.dll may go into an infinite loop when unpacking PE files. It is possible that this can crash the scanning engine **CVE ID : CVE-2022-28886**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-CLOU-101022/320
Product: collaboration_protection					
Affected Version(s): *					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Sep-2022	5.5	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.so/aerdl.dll may go into an infinite loop when unpacking PE files.	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-COLL-101022/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It is possible that this can crash the scanning engine **CVE ID : CVE-2022-28886**		
Product: elements_endpoint_protection					
Affected Version(s): *					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Sep-2022	5.5	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.so/aerdl.dll may go into an infinite loop when unpacking PE files. It is possible that this can crash the scanning engine **CVE ID : CVE-2022-28886**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-ELEM-101022/322
Product: internet_gatekeeper					
Affected Version(s): -					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Sep-2022	5.5	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.so/aerdl.dll may go into an infinite loop when unpacking PE files. It is possible that this can crash the scanning engine **CVE ID : CVE-2022-28886**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-INTE-101022/323
Product: linux_security					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
Loop with Unreachable Exit Condition ('Infinite Loop')	23-Sep-2022	5.5	A Denial-of-Service vulnerability was discovered in the F-Secure and WithSecure products where aerdl.so/aerdl.dll may go into an infinite loop when unpacking PE files. It is possible that this can crash the scanning engine **CVE ID : CVE-2022-28886**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-LINU-101022/324
Vendor: Fabasoft					
Product: fabasoft_cloud_enterprise_client					
Affected Version(s): 22.4.0043					
Improper Privilege Management	19-Sep-2022	7.8	The folioupdate service in Fabasoft Cloud Enterprise Client 22.4.0043 allows Local Privilege Escalation. **CVE ID : CVE-2022-29908**	N/A	A-FAB-FABA-101022/325
Vendor: fastly					
Product: js-compute					
Affected Version(s): * Up to (excluding) 0.5.3					
Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	20-Sep-2022	7.5	The JS Compute Runtime for Fastly's Compute@Edge platform provides the environment JavaScript is executed in when using the	https://github.com/fastly/js-compute-runtime/security/advisories/GHSA-cmr8-5w4c-44v8	A-FAS-JS-C-101022/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute@Edge JavaScript SDK. In versions prior to 0.5.3, the `Math.random` and `crypto.getRandomValues` methods fail to use sufficiently random values. The initial value to seed the PRNG (pseudorandom number generator) is baked-in to the final WebAssembly module, making the sequence of random values for that specific WebAssembly module predictable. An attacker can use the fixed seed to predict random numbers generated by these functions and bypass cryptographic security controls, for example to disclose sensitive data encrypted by functions that use these generators. The problem has been patched in version 0.5.3. No known workarounds exist. **CVE ID : CVE-2022-39218**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Fedoraproject					
Product: extra_packages_for_enterprise_linux					
Affected Version(s): 8.0					
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.com/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6903b9e41fe7cb70030e8750	A-FED-EXTR-101022/327
Affected Version(s): 9.0					
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.com/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6903b9e41fe7cb70030e8750	A-FED-EXTR-101022/328
Vendor: Ffmpeg					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ffmpeg					
Affected Version(s): 5.1					
Out-of-bounds Write	23-Sep-2022	7.8	A heap out-of-bounds memory write exists in FFMPEG since version 5.1. The size calculation in `build_open_gop_key_points()` goes through all entries in the loop and adds `sc->ctts_data[i].count` to `sc->sample_offsets_count`. This can lead to an integer overflow resulting in a small allocation with `av_calloc()`. An attacker can cause remote code execution via a malicious mp4 file. We recommend upgrading past commit c953baa084607dd1d84c3bfcce3cf6a87c3e6e05 **CVE ID : CVE-2022-2566**	https://github.com/FFmpeg/FFmpeg/commit/c953baa084607dd1d84c3bfcce3cf6a87c3e6e05	A-FFM-FFMP-101022/329
Vendor: Flatpress					
Product: flatpress					
Affected Version(s): 1.2.1					
Unrestricted Upload of File with	29-Sep-2022	7.2	Flatpress v1.2.1 was discovered to contain a remote code execution (RCE) vulnerability	N/A	A-FLA-FLAT-101022/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			in the Upload File function. **CVE ID : CVE-2022-40048**		
Vendor: food_ordering_management_system_project					
Product: food_ordering_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	9.8	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System. This affects an unknown part of the file router.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-209583. **CVE ID : CVE-2022-3332**	N/A	A-FOO-FOOD-101022/331
Vendor: Forgerock					
Product: ldap_connector					
Affected Version(s): * Up to (excluding) 1.5.20.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	19-Sep-2022	9.8	When the LDAP connector is started with StartTLS configured, unauthenticated access is granted. This issue affects: all versions of the LDAP connector prior to 1.5.20.9. The LDAP connector is bundled with Identity Management (IDM) and Remote Connector Server (RCS) **CVE ID : CVE-2022-0143**	https://backstage.forgerock.com/downloads/browse/idm/featured/connectors, https://backstage.forgerock.com/knowledge/kb/article/a11380515	A-FOR-LDAP-101022/332
Vendor: freehtmldesigns					
Product: site_offline					
Affected Version(s): * Up to (excluding) 1.5.3					
Authorization Bypass Through User-Controlled Key	19-Sep-2022	4.3	The Site Offline Or Coming Soon Or Maintenance Mode WordPress plugin before 1.5.3 prevents users from accessing a website but does not do so if the URL contained certain keywords. Adding those keywords to the URL's query string would bypass the plugin's main feature. **CVE ID : CVE-2022-1580**	N/A	A-FRE-SITE-101022/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: frrouting					
Product: frrouting					
Affected Version(s): * Up to (excluding) 8.4					
Out-of-bounds Read	19-Sep-2022	9.1	An out-of-bounds read in the BGP daemon of FRRouting FRR before 8.4 may lead to a segmentation fault and denial of service. This occurs in bgp_capability_msg_parse in bgpd/bgp_packet.c. **CVE ID : CVE-2022-37032**	https://bugzilla.suse.com/show_bug.cgi?id=1202023, https://github.com/FRRouting/frr/commit/6d58272b4cf96f0daa846210dd2104877900f921, https://github.com/FRRouting/frr/commit/ff6db1027f8f36df657ff2e5ea167773752537ed	A-FRR-FRRO-101022/334
Vendor: fullworksplugins					
Product: meet_my_team					
Affected Version(s): * Up to (including) 2.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Meet My Team plugin <= 2.0.5 at WordPress. **CVE ID : CVE-2022-37339**	https://patchstack.com/database/vulnerability/meet-my-team/wordpress-meet-my-team-plugin-2-0-5-authenticated-stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/meet-my-team/#developers	A-FUL-MEET-101022/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: fwupd					
Product: fwupd					
Affected Version(s): * Up to (excluding) 1.8.5					
Files or Directories Accessible to External Parties	28-Sep-2022	6.5	When creating an OPERATOR user account on the BMC, the redfish plugin saved the auto-generated password to /etc/fwupd/redfish.conf without proper restriction, allowing any user on the system to read the same configuration file. **CVE ID : CVE-2022-3287**	https://github.com/fwupd/fwupd/commit/ea676855f2119e36d433fbd2ed604039f53b2091	A-FWU-FWUP-101022/336
Vendor: Gajim					
Product: gajim					
Affected Version(s): * Up to (excluding) 1.5.0					
N/A	27-Sep-2022	5.3	An issue was discovered in Gajim through 1.4.7. The vulnerability allows attackers, via crafted XML stanzas, to correct messages that were not sent by them. The attacker needs to be part of the group chat or single chat. The fixed version is 1.5.0. **CVE ID : CVE-2022-39835**	https://dev.gajim.org/gajim/gajim/-/tags, https://dev.gajim.org/gajim/gajim/-/blob/master/ChangeLog	A-GAJ-GAJI-101022/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: garage_management_system_project					
Product: garage_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	16-Sep-2022	7.2	Garage Management System v1.0 is vulnerable to Arbitrary code execution via ip/garage/php_action/editProductImage.php?id=1. **CVE ID : CVE-2022-38877**	N/A	A-GAR-GARA-101022/338
Vendor: gavazziautomation					
Product: cpy_car_park_server					
Affected Version(s): * Up to (excluding) 2.8.3					
Use of Hard-coded Credentials	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials to gain full access to the device. **CVE ID : CVE-2022-22522**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/339
Missing Authentication for Critical Function	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a missing authentication allows for full access via API.	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22526		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could utilize an improper input validation on an API-submitted parameter to execute arbitrary OS commands. **CVE ID : CVE-2022-28811**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/341
Use of Hard-coded Credentials	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials to gain SuperUser access to the device. **CVE ID : CVE-2022-28812**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/342
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	9.8	Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 was discovered to be vulnerable to a relative path traversal	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability which enables remote attackers to read arbitrary files and gain full control of the device. **CVE ID : CVE-2022-28814**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	9.4	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 an unauthenticated remote attacker could utilize a SQL-Injection vulnerability to gain full database access, modify users and stop services . **CVE ID : CVE-2022-22524**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/344
Improper Authentication	28-Sep-2022	7.5	An improper authentication vulnerability exists in the Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 Web-App which allows an authentication bypass to the context of an unauthorised user if free-access is disabled. **CVE ID : CVE-2022-22523**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	28-Sep-2022	7.2	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 an remote attacker with admin rights could execute arbitrary commands due to missing input sanitization in the backup restore function **CVE ID : CVE-2022-22525**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/346
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	6.1	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 the Sentilo Proxy is prone to reflected XSS which only affects the Sentilo service. **CVE ID : CVE-2022-28816**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/347
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	5.3	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of an SQL-injection to gain access to a volatile temporary database with the	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current states of the device. **CVE ID : CVE-2022-28813**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	2.7	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 the Sentilo Proxy server was discovered to contain a SQL injection vulnerability allowing an attacker to query other tables of the Sentilo service. **CVE ID : CVE-2022-28815**	https://cert.vde.com/en/advisories/VDE-2022-029/	A-GAV-CPY_-101022/349
Vendor: genesys					
Product: pureconnect					
Affected Version(s): * Up to (including) 2022-09-26					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	6.1	Genesys PureConnect Interaction Web Tools Chat Service (up to at least 26-September- 2019) allows XSS within the Printable Chat History via the participant -> name JSON POST parameter. **CVE ID : CVE-2022-37775**	https://help.genesys.com/pureconnect/mergedprojects/wh_tr/desktop/pdfs/web_tools_dg.pdf	A-GEN-PURE-101022/350
Vendor: getawesomesupport					
Product: awesome_support					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 6.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Multiple Authenticated (custom specific plugin role) Persistent Cross-Site Scripting (XSS) vulnerability in Awesome Support plugin <= 6.0.7 at WordPress. **CVE ID : CVE-2022-38073**	https://wordpress.org/plugins/awesome-support/#developers, https://patchstack.com/database/vulnerability/awesome-support/wordpress-awesome-support-plugin-6-0-7-multiple-authenticated-stored-cross-site-scripting-xss-vulnerabilities	A-GET-AWES-101022/351
Vendor: gettext_override_translations_project					
Product: gettext_override_translations					
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	4.8	The Gettext override translations WordPress plugin before 2.0.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	A-GET-GETT-101022/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3036		
Vendor: ghas-to-csv_project					
Product: ghas-to-csv					
Affected Version(s): * Up to (excluding) 1					
N/A	17-Sep-2022	9.8	some-natalie/ghas-to-csv (GitHub Advanced Security to CSV) is a GitHub action which scrapes the GitHub Advanced Security API and shoves it into a CSV. In affected versions this GitHub Action creates a CSV file without sanitizing the output of the APIs. If an alert is dismissed or any other custom field contains executable code / formulas, it might be run when an endpoint opens that CSV file in a spreadsheet program. This issue has been addressed in version `v1`. Users are advised to use `v1` or later. There are no known workarounds for this issue. **CVE ID : CVE-2022-39217**	https://github.com/some-natalie/ghas-to-csv/commit/d0b521928fa734513b5cd9c7d9d8e09db50e884a, https://github.com/some-natalie/ghas-to-csv/security/advisories/GHSA-634p-93h9-92vh	A-GHA-GHAS-101022/353
Vendor: globalnorthstar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: northstar_club_management					
Affected Version(s): 6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	There are two full (read/write) Blind/Time-based SQL injection vulnerabilities in the Northstar Club Management version 6.3 application. The vulnerabilities exist in the userName parameter of the processlogin.jsp page in the /northstar/Portal/ directory and the userID parameter of the login.jsp page in the /northstar/iphone/ directory. Exploitation of the SQL injection vulnerabilities allows full access to the database which contains critical data for organization's that make full use of the software suite. **CVE ID : CVE-2022-26959**	N/A	A-GLO-NORT-101022/354
Vendor: Glpi-project					
Product: glpi					
Affected Version(s): * Up to (including) 10.0.2					
Improper Neutralization of	19-Sep-2022	9.8	/vendor/htmlawed/htmlawed/htmLawedTest.php in the	http://www.bioinformatics.org/phplabware/s	A-GLP-GLPI-101022/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			htmlawed module for GLPI through 10.0.2 allows PHP code injection. **CVE ID : CVE-2022-35914**	ourceer/sourceer.php?&Sfs=htmLawedTest.php&Sl=.%2Finternal_utilities%2FhtmLawed, https://glpi-project.org/fr/glpi-10-0-3-disponible/	
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 104.0.5112.101					
Use After Free	26-Sep-2022	8.8	Use after free in FedCM in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2852**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1349322	A-GOO-CHRO-101022/356
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Downloads in Google Chrome on Android prior to 104.0.5112.101 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2853**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1350097	A-GOO-CHRO-101022/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	8.8	Use after free in SwiftShader in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2854**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1337538	A-GOO-CHRO-101022/358
Use After Free	26-Sep-2022	8.8	Use after free in ANGLE in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2855**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1345042	A-GOO-CHRO-101022/359
Use After Free	26-Sep-2022	8.8	Use after free in Blink in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2857**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1338135	A-GOO-CHRO-101022/360
Use After Free	26-Sep-2022	8.8	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.101	https://chromereleases.googleblog.com/2022/08/stable-channel-update-	A-GOO-CHRO-101022/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via specific UI interaction. **CVE ID : CVE-2022-2858**	for-desktop_16.html, https://crbug.com/1341918	
Use After Free	26-Sep-2022	8.8	Use after free in Chrome OS Shell in Google Chrome prior to 104.0.5112.101 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2859**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1338412	A-GOO-CHRO-101022/362
Use After Free	26-Sep-2022	8.8	Use after free in Browser Creation in Google Chrome prior to 104.0.5112.101 allowed a remote attacker who had convinced a user to engage in a specific UI interaction to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2998**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1329794	A-GOO-CHRO-101022/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	26-Sep-2022	6.5	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 104.0.5112.101 allowed a remote attacker to arbitrarily browse to a malicious website via a crafted HTML page. **CVE ID : CVE-2022-2856**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1345630	A-GOO-CHRO-101022/364
N/A	26-Sep-2022	6.5	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to bypass cookie prefix restrictions via a crafted HTML page. **CVE ID : CVE-2022-2860**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1345193	A-GOO-CHRO-101022/365
Incorrect Authorization	26-Sep-2022	6.5	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.101 allowed an attacker who convinced a user to install a malicious extension to inject arbitrary scripts into WebUI via a crafted HTML page.	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1346236	A-GOO-CHRO-101022/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2861		
Affected Version(s): * Up to (excluding) 105.0.5195.102					
Improper Input Validation	26-Sep-2022	9.6	Insufficient data validation in Mojo in Google Chrome prior to 105.0.5195.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2022-3075**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html	A-GOO-CHRO-101022/367
Affected Version(s): * Up to (excluding) 105.0.5195.125					
Out-of-bounds Write	26-Sep-2022	8.8	Out of bounds write in Storage in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. **CVE ID : CVE-2022-3195**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1358381	A-GOO-CHRO-101022/368
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	https://crbug.com/1358090, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html	A-GOO-CHRO-101022/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3196		
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3197**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1358075	A-GOO-CHRO-101022/370
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3198**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1355682	A-GOO-CHRO-101022/371
Use After Free	26-Sep-2022	8.8	Use after free in Frames in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3199**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1355237	A-GOO-CHRO-101022/372
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Internals in Google Chrome prior to	https://crbug.com/1355103, https://chromereleases.google	A-GOO-CHRO-101022/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3200**	blog.com/2022/09/stable-channel-update-for-desktop_14.html	
Improper Input Validation	26-Sep-2022	5.4	Insufficient validation of untrusted input in DevTools in Google Chrome on Chrome OS prior to 105.0.5195.125 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2022-3201**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1343104	A-GOO-CHRO-101022/374
Affected Version(s): * Up to (excluding) 105.0.5195.52					
Use After Free	26-Sep-2022	8.8	Use after free in Network Service in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3038**	https://crbug.com/1340253, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	8.8	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3039**	https://crbug.com/1343348, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/376
Use After Free	26-Sep-2022	8.8	Use after free in Layout in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3040**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1341539	A-GOO-CHRO-101022/377
Use After Free	26-Sep-2022	8.8	Use after free in WebSQL in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3041**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1345947	A-GOO-CHRO-101022/378
Use After Free	26-Sep-2022	8.8	Use after free in PhoneHub in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-	A-GOO-CHRO-101022/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3042**	desktop_30.html, https://crbug.com/1338553	
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Screen Capture in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3043**	https://crbug.com/1336979, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/380
Incorrect Authorization	26-Sep-2022	8.8	Insufficient validation of untrusted input in V8 in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3045**	https://crbug.com/1339648, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/381
Use After Free	26-Sep-2022	8.8	Use after free in Browser Tag in Google Chrome prior to	https://chromereleases.googleblog.com/2022/08/stable-	A-GOO-CHRO-101022/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			105.0.5195.52 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3046**	channel-update-for-desktop_30.html, https://crbug.com/1346245	
Use After Free	26-Sep-2022	8.8	Use after free in SplitScreen in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3049**	https://crbug.com/1316892, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/383
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in WebUI in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1337132	A-GOO-CHRO-101022/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via crafted UI interactions. **CVE ID : CVE-2022-3050**		
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Exosphere in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3051**	https://crbug.com/1345245, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/385
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Window Manager in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3052**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1346154	A-GOO-CHRO-101022/386
Use After Free	26-Sep-2022	8.8	Use after free in Passwords in	https://crbug.com/1351969,	A-GOO-CHRO-101022/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3055**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	
Use After Free	26-Sep-2022	8.8	Use after free in Sign-In Flow in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interaction. **CVE ID : CVE-2022-3058**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1337676	A-GOO-CHRO-101022/388
Use After Free	26-Sep-2022	8.8	Use after free in Tab Strip in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption	https://crbug.com/1333995, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via crafted UI interaction. **CVE ID : CVE-2022-3071**		
Missing Authorization	26-Sep-2022	6.8	Inappropriate implementation in Chrome OS lockscreen in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a local attacker to bypass lockscreen navigation restrictions via physical access to the device. **CVE ID : CVE-2022-3048**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1303308	A-GOO-CHRO-101022/390
Incorrect Authorization	26-Sep-2022	6.5	Inappropriate implementation in Site Isolation in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2022-3044**	https://crbug.com/1051198, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-CHRO-101022/391
Incorrect Authorization	26-Sep-2022	6.5	Insufficient policy enforcement in Extensions API in Google Chrome prior to 105.0.5195.52 allowed an attacker	https://crbug.com/1342586, https://chromereleases.googleblog.com/2022/08/stable-channel-update-	A-GOO-CHRO-101022/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who convinced a user to install a malicious extension to bypass downloads policy via a crafted HTML page. **CVE ID : CVE-2022-3047**	for-desktop_30.html	
N/A	26-Sep-2022	6.5	Insufficient policy enforcement in DevTools in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3054**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1290236	A-GOO-CHRO-101022/393
Incorrect Authorization	26-Sep-2022	6.5	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2022-3056**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1329460	A-GOO-CHRO-101022/394
Incorrect Authorization	26-Sep-2022	6.5	Inappropriate implementation in iframe Sandbox in Google Chrome prior to 105.0.5195.52 allowed a remote	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.htm	A-GOO-CHRO-101022/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2022-3057**	l, https://crbug.com/1336904	
N/A	26-Sep-2022	4.3	Inappropriate implementation in Pointer Lock in Google Chrome on Mac prior to 105.0.5195.52 allowed a remote attacker to restrict user navigation via a crafted HTML page. **CVE ID : CVE-2022-3053**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1267867	A-GOO-CHRO-101022/396
Product: lacros					
Affected Version(s): -					
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Exosphere in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3051**	https://crbug.com/1345245, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	A-GOO-LACR-101022/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Window Manager in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3052**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1346154	A-GOO-LACR-101022/398
Product: protobuf-cpp					
Affected Version(s): * Up to (excluding) 3.18.3					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially crafted message with multiple key-value per elements	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Affected Version(s): From (including) 3.19.0 Up to (excluding) 3.19.5					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially crafted message with multiple key-	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially crafted message	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Affected Version(s): From (including) 3.21.0 Up to (excluding) 3.21.6					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Product: protobuf-python					
Affected Version(s): * Up to (excluding) 3.18.3					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-python can lead to	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out of memory failures. A specially crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Affected Version(s): From (including) 3.19.0 Up to (excluding) 3.19.5					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5 for protobuf-	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			python can lead to out of memory failures. A specially crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Affected Version(s): From (including) 3.20.0 Up to (excluding) 3.20.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 4.21.5	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for protobuf-python can lead to out of memory failures. A specially crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.21.6					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	7.5	A parsing vulnerability for the MessageSet type in the ProtocolBuffers versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4, 3.20.1 and 3.21.5 for protobuf-cpp, and versions prior to and including 3.16.1, 3.17.3, 3.18.2, 3.19.4,	https://cloud.google.com/support/bulletins#GCP-2022-019, https://github.com/protocolbuffers/protobuf/security/advisories/GHSA-8gq9-2x98-w8hf	A-GOO-PROT-101022/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.20.1 and 4.21.5 for protobuf-python can lead to out of memory failures. A specially crafted message with multiple key-value per elements creates parsing issues, and can lead to a Denial of Service against services receiving unsanitized input. We recommend upgrading to versions 3.18.3, 3.19.5, 3.20.2, 3.21.6 for protobuf-cpp and 3.18.3, 3.19.5, 3.20.2, 4.21.6 for protobuf-python. Versions for 3.16 and 3.17 are no longer updated. **CVE ID : CVE-2022-1941**		
Product: tensorflow					
Affected Version(s): * Up to (excluding) 2.7.2					
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedRelu` or `QuantizedRelu6` are given nonscalar inputs for `min_features` or `max_features`, it results in a segfault that can be used to	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v7vw-577f-vp8x, https://github.com/tensorflow/tensorflow/commit/49b3824d83af706df0ad07	A-GOO-TENS-101022/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35979**	e4e677d88659756d89	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `FractionalMaxPoolGrad` validates its inputs with `CHECK` failures instead of with returning errors. If it gets incorrectly sized inputs, the `CHECK` failure can be used to trigger a denial of service attack. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/8741e57d163a079db05a7107a7609af70931def4, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vxv8-r8q2-63xw	A-GOO-TENS-101022/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8741e57d163a079db05a7107a7609af70931def4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35981**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `SparseBincount` is given inputs for `indices`, `values`, and `dense_shape` that do not make a valid sparse tensor, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 40adbe4dd15b582b0210dfbf40c243a62f5119fa. The fix will be included in TensorFlow 2.10.0. We will also	https://github.com/tensorflow/tensorflow/commit/40adbe4dd15b582b0210dfbf40c243a62f5119fa, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-397c-5g2j-qxpv	A-GOO-TENS-101022/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35982**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Save` or `SaveSlices` is run over tensors of an unsupported `dtype`, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6vp-8q9j-whx4, https://github.com/tensorflow/tensorflow/commit/5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4	A-GOO-TENS-101022/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35983**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `ParameterizedTruncatedNormal` assumes `shape` is of type `int32`. A valid `shape` of type `int64` results in a mismatched type `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 72180be03447a10810edca700cbc9af690dfeb51. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/72180be03447a10810edca700cbc9af690dfeb51, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p2xf-8hgm-hpw5	A-GOO-TENS-101022/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35984		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LRNGrad` is given an `output_image` input tensor that is not 4-D, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bd90b3efab4ec958b228cd7cfe9125be1c0cf255. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35985**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9942-r22v-78cp, https://github.com/tensorflow/tensorflow/commit/bd90b3efab4ec958b228cd7cfe9125be1c0cf255	A-GOO-TENS-101022/412
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If	https://github.com/tensorflow/tensorflow/commit/7a4591fd4f065f4fa903593	A-GOO-TENS-101022/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`RaggedBincount` is given an empty input tensor `splits`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7a4591fd4f065f4fa903593bc39b2f79530a74b8. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35986**	bc39b2f79530a74b8, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wr9v-g9vf-c74v	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `DenseBincount` assumes its input tensor `weights` to either have the same shape as its input tensor `input` or to be length-0. A different `weights` shape will trigger a	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-w62h-8xjm-fv49, https://github.com/tensorflow/tensorflow/commit/bf4c14353c2328636a18bfad1e151052c81d5f43	A-GOO-TENS-101022/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf4c14353c2328636a18bfad1e151052c81d5f43. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35987**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.linalg.matrix_rank` receives an empty input `a`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9vqj-64pv-w55c	A-GOO-TENS-101022/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35988**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `MaxPool` receives a window size input array `ksize` with dimensions greater than its input tensor `input`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 32d7bd3defd134f21a4e344c8dfd400999aaf6b18. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/32d7bd3defd134f21a4e344c8dfd40099aaf6b18, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j43h-pgmg-5hjq	A-GOO-TENS-101022/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35989**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_per_channel_gradient` receives input `min` or `max` of rank other than 1, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h7ff-cfc9-wmmh, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319feed	A-GOO-TENS-101022/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range.There are no known workarounds for this issue. **CVE ID : CVE-2022-35990**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListScatter` and `TensorListScatterV2` receive an `element_shape` of a rank greater than one, they give a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit bb03fdf4aae944ab2e4b35c7daa051068a8b7f61. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/commit/bb03fdf4aae944ab2e4b35c7daa051068a8b7f61, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vm7x-4qhj-rrcq	A-GOO-TENS-101022/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35991**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListFromTensor` receives an `element_shape` of a rank greater than one, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 3db59a042a38f4338aa207922fa2f476e000a6ee. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35992**	https://github.com/tensorflow/tensorflow/commit/3db59a042a38f4338aa207922fa2f476e000a6ee, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9v8w-xmr4-wgxp	A-GOO-TENS-101022/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `SetSize` receives an input `set_shape` that is not a 1D tensor, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit cf70b79d2662c0d3c6af74583641e345fc939467. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35993**	https://github.com/tensorflow/tensorflow/commit/cf70b79d2662c0d3c6af74583641e345fc939467, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wq6q-6m32-9rv9	A-GOO-TENS-101022/420
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `CollectiveGather` receives an scalar input `input`, it	https://github.com/tensorflow/tensorflow/commit/c1f491817dec39a26be3c574e86a88c30f3c4770, https://github.c	A-GOO-TENS-101022/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c1f491817dec39a26be3c574e86a88c30f3c4770. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35994**	om/tensorflow/tensorflow/security/advisories/GHSA-fhfc-2q7x-929f	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `AudioSummaryV2` receives an input `sample_rate` with more than one element, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9h5-vr8m-x2h4, https://github.com/tensorflow/tensorflow/commit/bf6b45244992e2ee543c258e519489659c99fb7f	A-GOO-TENS-101022/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit bf6b45244992e2ee543c258e519489659c99fb7f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35995**		
Divide By Zero	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Conv2D` is given empty `input` and the `filter` and `padding` sizes are valid, the output is all-zeros. This causes division-by-zero floating point exceptions that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 611d80db29dd7b0cfb755772c69d60ae5bca05f9. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/611d80db29dd7b0cfb755772c69d60ae5bca05f9, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q5jv-m6qw-5g37	A-GOO-TENS-101022/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35996**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `tf.sparse.cross` receives an input `separator` that is not a scalar, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 83dcb4dbfa094e33db084e97c4d0531a559e0ebf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p7hr-f446-x6qf, https://github.com/tensorflow/tensorflow/commit/83dcb4dbfa094e33db084e97c4d0531a559e0ebf	A-GOO-TENS-101022/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35997**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `EmptyTensorList` receives an input `element_shape` with more than one dimension, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c8ba76d48567aed347508e0552a257641931024d. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qhw4-wwr7-gjc5, https://github.com/tensorflow/tensorflow/commit/c8ba76d48567aed347508e0552a257641931024d	A-GOO-TENS-101022/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35998		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Conv2DBackpropInput` receives empty `out_backprop` inputs (e.g. `[3, 1, 0, 1]`), the current CPU/GPU kernels `CHECK` fail (one with dnnl, the other with cudnn). This can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 27a65a43cf763897fecfa5cdb5cc653fc5dd0346. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35999**	https://github.com/tensorflow/tensorflow/commit/27a65a43cf763897fecfa5cdb5cc653fc5dd0346, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-37jf-mjv6-xfqw	A-GOO-TENS-101022/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit aed36912609fc07229b4d0a7b44f3f48efc00fd0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36000**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqxc-pvf8-2w9v, https://github.com/tensorflow/tensorflow/commit/aed36912609fc07229b4d0a7b44f3f48efc00fd0	A-GOO-TENS-101022/427
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `DrawBoundingBoxes` receives an input `boxes` that	https://github.com/tensorflow/tensorflow/commit/da0d65cdc1270038e72157ba35bf74b85d9bda11, https://github.c	A-GOO-TENS-101022/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is not of dtype `float`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit da0d65cdc1270038e72157ba35bf74b85d9bda11. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36001**	om/tensorflow/tensorflow/security/advisories/GHSA-jqm7-m5q7-3hm5	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Unbatch` receives a nonscalar input `id`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 4419d10d576adef	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mh3m-62v7-68xg, https://github.com/tensorflow/tensorflow/commit/4419d10d576adefa36b0e0a9425d2569f7c0189f	A-GOO-TENS-101022/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a36b0e0a9425d2569f7c0189f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36002**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RandomPoissonV2` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cv2p-32v3-vhwq, https://github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3	A-GOO-TENS-101022/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36003**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.random.gamma` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv8m-8x97-937q	A-GOO-TENS-101022/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-36004**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_gradient` receives input `min` or `max` that is nonscalar, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36005**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-r26c-679w-mrjm, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319feed	A-GOO-TENS-101022/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit 1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36011**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fv43-93gv-vm8f, https://github.com/tensorflow/tensorflow/commit/1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b	A-GOO-TENS-101022/433
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jvhc-5hhr-w3v5, https://github.com/tensorflow/	A-GOO-TENS-101022/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			given empty function attributes, it crashes. We have patched the issue in GitHub commit ad069af92392efee1418c48ff561fd3070a03d7b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36012**	tensorflow/commit/ad069af92392efee1418c48ff561fd3070a03d7b	
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::GraphDefImporter::ConvertNodeDef` tries to convert NodeDefs without an op name, it crashes. We have patched the issue in GitHub commit a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-828c-5j5q-vrjq	A-GOO-TENS-101022/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36013**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::TFOp::nameAttr` receives null type list attributes, it crashes. We have patched the issue in GitHub commits 3a754740d5414e362512ee981eefba41561a63a6 and a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7j3m-8g3c-9qqq	A-GOO-TENS-101022/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36014**		
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RangeSize` receives values that do not fit into an `int64_t`, it crashes. We have patched the issue in GitHub commit 37e64539cd29fcfb814c4451152a60f5d107b0f0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36015**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rh87-q4vg-m45j, https://github.com/tensorflow/tensorflow/commit/37e64539cd29fcfb814c4451152a60f5d107b0f0	A-GOO-TENS-101022/437
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning.	https://github.com/tensorflow/tensorflow/commit/6104f0d40	A-GOO-TENS-101022/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When `tensorflow::full_type::SubstituteFromAttrs` receives a `FullTypeDef& t` that is not exactly three args, it triggers a `CHECK`-fail instead of returning a status. We have patched the issue in GitHub commit 6104f0d4091c260ce9352f9155f7e9b725eab012. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36016**	91c260ce9352f9155f7e9b725eab012, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g468-qj8g-vcjc	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Requantize` is given `input_min`, `input_max`, `requested_output_min`, `requested_output_	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/sec	A-GOO-TENS-101022/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36017**	urity/advisories/GHSA-wqmc-pm8c-2jhc	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedTensorToVariant` is given a `rt_nested_splits` list that contains tensors of ranks other than one, it results in a `CHECK` fail that can be used to	https://github.com/tensorflow/tensorflow/commit/88f93dfe691563baa4ae1e80ccde2d5c7a143821, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6cv-4fmf-66xf	A-GOO-TENS-101022/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger a denial of service attack. We have patched the issue in GitHub commit 88f93dfe691563baa4ae1e80ccde2d5c7a143821. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36018**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVarsPerChannel` is given `min` or `max` tensors of a rank other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9j4v-pp28-mxv7	A-GOO-TENS-101022/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36019**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizeAndDequantizeV3` is given a nonscalar `num_bits` input tensor, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit f3f9cb38ecfe5a8a703f2c4a8fead434ef291713. The fix will be included in TensorFlow 2.10.0. We will also	https://github.com/tensorflow/tensorflow/commit/f3f9cb38ecfe5a8a703f2c4a8fead434ef291713, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9cr2-8pwr-fhfq	A-GOO-TENS-101022/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36026**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When converting transposed convolutions using per-channel weight quantization the converter segfaults and crashes the Python process. We have patched the issue in GitHub commit aa0b852a4588cea4d36b74feb05d93055540b450. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/commit/aa0b852a4588cea4d36b74feb05d93055540b450, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-79h2-q768-fpxr	A-GOO-TENS-101022/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36027**		
Affected Version(s): 2.10					
Out-of-bounds Write	16-Sep-2022	9.8	TensorFlow is an open source platform for machine learning. The `ScatterNd` function takes an input argument that determines the indices of of the output tensor. An input index greater than the output tensor or less than zero will either write content at the wrong index or trigger a crash. We have patched the issue in GitHub commit b4d4b4cb019bd7240a52daa4ba61e3cc814f0384. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/b4d4b4cb019bd7240a52daa4ba61e3cc814f0384, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-ffjm-4qwc-7cmf	A-GOO-TENS-101022/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-35939**		
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. This issue has been patched in GitHub commit 4142e47e9e31db481781b955ed3ff807a781b494. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tflite-micro/commit/4142e47e9e31db481781b955ed3ff807a781b494, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-3m3g-pf5v-5hpj	A-GOO-TENS-101022/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35938		
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read is triggered. This issue has been patched in GitHub commit 595a65a3e224a0362d7e68c2213acfc2b499a196. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35937**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pxrw-j2fv-hx3h, https://github.com/tensorflow/tensorflow/commit/595a65a3e224a0362d7e68c2213acfc2b499a196	A-GOO-TENS-101022/446
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source	https://github.com/tensorflow/	A-GOO-TENS-101022/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			platform for machine learning. The implementation of tf.reshape op in TensorFlow is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by overflowing the number of elements in a tensor. This issue has been patched in GitHub commit 61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35934**	tensorflow/commit/61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f4w6-h4f5-wx45	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-97p7-w86h-vcf9,	A-GOO-TENS-101022/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SobolSampleOp is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by assuming `input(0)`, `input(1)`, and `input(2)` to be scalar. This issue has been patched in GitHub commit c65c67f88ad770662e8f191269a907bf2b94b1bf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35935**	https://github.com/tensorflow/tensorflow/commit/c65c67f88ad770662e8f191269a907bf2b94b1bf	
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `RaggedRangOp` function takes an argument `limits` that is eventually used to construct a	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-x989-q2pq-4q5x, https://github.com/tensorflow/tensorflow/commit/37cefa91be	A-GOO-TENS-101022/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`TensorShape` as an `int64`. If `limits` is a very large float, it can overflow when converted to an `int64`. This triggers an `InvalidArgument` but also throws an abort signal that crashes the program. We have patched the issue in GitHub commit 37cefa91bee4eace55715eeef43720b958a01192. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35940**	e4eace55715eeef43720b958a01192	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `AvgPoolOp` function takes an argument `ksize` that must be positive but is not	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/	A-GOO-TENS-101022/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checked. A negative `ksize` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds to this issue. **CVE ID : CVE-2022-35941**	tensorflow/security/advisories/GHSA-mgmh-g2v6-mqw5	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `UnbatchGradOp` function takes an argument `id` that is assumed to be a scalar. A nonscalar `id` can trigger a `CHECK` failure and crash the program. It also requires its	https://github.com/tensorflow/tensorflow/commit/5f945fc6409a3c1e90d6970c9292f805f6e6ddf2, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h5vq-gw2c-pq47	A-GOO-TENS-101022/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument `batch_index` to contain three times the number of elements as indicated in its `batch_index.dim_size(0)`. An incorrect `batch_index` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 5f945fc6409a3c1e90d6970c9292f805f6e6ddf2. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35952**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPool3DGradOp` does not fully	https://github.com/tensorflow/tensorflow/commit/9178ac9d6389bdc54638ab913ea0e419234d14eb, https://github.c	A-GOO-TENS-101022/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the input `orig_input_shape`. This results in an overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 9178ac9d6389bdc54638ab913ea0e419234d14eb. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35959**	om/tensorflow/tensorflow/security/advisories/GHSA-wxjj-cgcx-r3vq	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. In `core/kernels/list_kernels.cc's TensorListReserve`, `num_elements` is assumed to be a tensor of size 1.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v5xg-3q2c-c2r4, https://github.com/tensorflow/tensorflow/commit/b5f6fbfba76576202b7211	A-GOO-TENS-101022/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When a `num_elements` of more than 1 element is provided, then `tf.raw_ops.TensorListReserve` fails the `CHECK_EQ` in `CheckIsAlignedAndSingleElement`. We have patched the issue in GitHub commit b5f6fbfba76576202b72119897561e3bd4f179c7. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35960**	9897561e3bd4f179c7	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `FractionalAvgPoolGrad` does not fully validate the input `orig_input_tensor_`	https://github.com/tensorflow/tensorflow/commit/03a659d7be9a1154fdf5eeac221e5950fec07dad, https://github.com/tensorflow/tensorflow/sec	A-GOO-TENS-101022/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shape`. This results in an overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 03a659d7be9a1154fdf5eeac221e5950fec07dad. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35963**	urity/advisories/GHSA-84jm-4cf3-9jfm	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `BlockLSTMGradV2` does not fully validate its inputs. This results in a a segfault that can be used to trigger a denial of service	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f7r5-q7cx-h668, https://github.com/tensorflow/tensorflow/commit/2a458fc4866505be27c62f81474ecb2b870498fa	A-GOO-TENS-101022/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack. We have patched the issue in GitHub commit 2a458fc4866505be27c62f81474ecb2b870498fa. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35964**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LowerBound` or `UpperBound` is given an empty`sorted_inputs` input, it results in a `nullptr` dereference, leading to a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bce3717eaef4f769019fd18e990464ca	https://github.com/tensorflow/tensorflow/commit/bce3717eaef4f769019fd18e990464ca4a2efeea, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qxpx-j395-pw36	A-GOO-TENS-101022/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4a2efeea. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35965**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedAvgPool` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7cdf9d4d2083b739ec81cfdace546b0c99f50622. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this	https://github.com/tensorflow/tensorflow/commit/7cdf9d4d2083b739ec81cfdace546b0c99f50622, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4w68-4x85-mjj9	A-GOO-TENS-101022/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35966**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedAdd` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v6h3-348g-6h5x, https://github.com/tensorflow/tensorflow/commit/49b3824d83af706df0ad07e4e677d88659756d89	A-GOO-TENS-101022/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35967**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPoolGrad` does not fully validate the input `orig_input_shape`. This results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-2475-53vw-vp25	A-GOO-TENS-101022/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35968		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `Conv2DBackpropInput` requires `input_sizes` to be 4-dimensional. Otherwise, it gives a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 50156d547b9a1da0144d7babe665cf690305b33c. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35969**	https://github.com/tensorflow/tensorflow/commit/50156d547b9a1da0144d7babe665cf690305b33c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q2c3-jpmc-gfjx	A-GOO-TENS-101022/460
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for	https://github.com/tensorflow/tensorflow/com	A-GOO-TENS-101022/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine learning. If `QuantizedInstanceNorm` is given `x_min` or `x_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35970**	mit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g35r-369w-3fqp	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVars` is given `min` or `max` tensors of a	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/	A-GOO-TENS-101022/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nonzero rank, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35971**	tensorflow/security/advisories/GHSA-9fpg-838v-wpv7	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedBiasAdd` is given `min_input`, `max_input`, `min_bias`, `max_bias` tensors of a nonzero rank, it results in a segfault that can be	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4pc4-m9mj-v2r9	A-GOO-TENS-101022/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35972**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedMatMul` is given nonscalar input for: `min_a`, `max_a`, `min_b`, or `max_b` It gives a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit aca766ac7693bf29ed0df55ad6bfcc78f	https://github.com/tensorflow/tensorflow/commit/aca766ac7693bf29ed0df55ad6bfcc78f35e7f48, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-689c-r7h2-fv9v	A-GOO-TENS-101022/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35e7f48. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35973**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizeDownAndShrinkRange` is given nonscalar inputs for `input_min` or `input_max`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 73ad1815ebcfeb7c051f9c2f7ab5024380ca8613. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vgvh-2pf4-jr2x, https://github.com/tensorflow/tensorflow/commit/73ad1815ebcfeb7c051f9c2f7ab5024380ca8613	A-GOO-TENS-101022/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35974**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedRelu` or `QuantizedRelu6` are given nonscalar inputs for `min_features` or `max_features`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v7vw-577f-vp8x, https://github.com/tensorflow/tensorflow/commit/49b3824d83af706df0ad07e4e677d88659756d89	A-GOO-TENS-101022/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35979**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `FractionalMaxPoolGrad` validates its inputs with `CHECK` failures instead of with returning errors. If it gets incorrectly sized inputs, the `CHECK` failure can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 8741e57d163a079db05a7107a7609af70931def4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/8741e57d163a079db05a7107a7609af70931def4, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vxv8-r8q2-63xw	A-GOO-TENS-101022/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-35981**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `SparseBincount` is given inputs for `indices`, `values`, and `dense_shape` that do not make a valid sparse tensor, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 40adbe4dd15b582b0210dfbf40c243a62f5119fa. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35982**	https://github.com/tensorflow/tensorflow/commit/40adbe4dd15b582b0210dfbf40c243a62f5119fa, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-397c-5g2j-qxpv	A-GOO-TENS-101022/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Save` or `SaveSlices` is run over tensors of an unsupported `dtype`, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35983**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6vp-8q9j-whx4, https://github.com/tensorflow/tensorflow/commit/5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4	A-GOO-TENS-101022/469
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `ParameterizedTruncatedNormal` assumes `shape` is	https://github.com/tensorflow/tensorflow/commit/72180be03447a10810edca700cbc9af690dfeb51,	A-GOO-TENS-101022/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of type `int32`. A valid `shape` of type `int64` results in a mismatched type `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 72180be03447a10810edca700cbc9af690dfeb51. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35984**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p2xf-8hgm-hpw5	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LRNGrad` is given an `output_image` input tensor that is not 4-D, it results in a `CHECK` fail that can be used to trigger a denial of	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9942-r22v-78cp, https://github.com/tensorflow/tensorflow/commit/bd90b3efab4ec958b228cd	A-GOO-TENS-101022/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service attack. We have patched the issue in GitHub commit bd90b3efab4ec958b228cd7cfe9125be1c0cf255. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35985**	7cfe9125be1c0cf255	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedBincount` is given an empty input tensor `splits`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7a4591fd4f065f4fa903593bc39b2f79530a74b8. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/7a4591fd4f065f4fa903593bc39b2f79530a74b8, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wr9v-g9vf-c74v	A-GOO-TENS-101022/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35986**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `DenseBincount` assumes its input tensor `weights` to either have the same shape as its input tensor `input` or to be length-0. A different `weights` shape will trigger a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf4c14353c2328636a18bfad1e1510 52c81d5f43. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-w62h-8xjm-fv49, https://github.com/tensorflow/tensorflow/commit/bf4c14353c2328636a18bfad1e151052c81d5f43	A-GOO-TENS-101022/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35987**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.linalg.matrix_rank` receives an empty input `a`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/commit/c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9vqj-64pv-w55c	A-GOO-TENS-101022/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35988**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `MaxPool` receives a window size input array `ksize` with dimensions greater than its input tensor `input`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 32d7bd3defd134f21a4e344c8dfd400999aaf6b18. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/32d7bd3defd134f21a4e344c8dfd40099aaf6b18, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j43h-pgmg-5hjq	A-GOO-TENS-101022/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35989		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_per_channel_gradient` receives input `min` or `max` of rank other than 1, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range.There are no known workarounds for this issue. **CVE ID : CVE-2022-35990**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h7ff-cfc9-wmmh, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319feed	A-GOO-TENS-101022/476
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for	https://github.com/tensorflow/tensorflow/com	A-GOO-TENS-101022/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine learning. When `TensorListScatter` and `TensorListScatterV2` receive an `element_shape` of a rank greater than one, they give a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit bb03fdf4aae944ab2e4b35c7daa05106 8a8b7f61. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35991**	mit/bb03fdf4aae944ab2e4b35c7daa051068a8b7f61, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vm7x-4qhj-rrcq	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListFromTensor` receives an `element_shape` of	https://github.com/tensorflow/tensorflow/commit/3db59a042a38f4338aa207922fa2f476e000a6ee, https://github.c	A-GOO-TENS-101022/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a rank greater than one, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 3db59a042a38f4338aa207922fa2f476e000a6ee. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35992**	om/tensorflow/tensorflow/security/advisories/GHSA-9v8w-xmr4-wgxp	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `SetSize` receives an input `set_shape` that is not a 1D tensor, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/cf70b79d2662c0d3c6af74583641e345fc939467, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wq6q-6m32-9rv9	A-GOO-TENS-101022/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cf70b79d2662c0d3c6af74583641e345fc939467. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35993**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `CollectiveGather` receives an scalar input `input`, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c1f491817dec39a26be3c574e86a88c30f3c4770. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on	https://github.com/tensorflow/tensorflow/commit/c1f491817dec39a26be3c574e86a88c30f3c4770, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fhfc-2q7x-929f	A-GOO-TENS-101022/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35994**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `AudioSummaryV2` receives an input `sample_rate` with more than one element, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf6b45244992e2ee543c258e519489659c99fb7f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9h5-vr8m-x2h4, https://github.com/tensorflow/tensorflow/commit/bf6b45244992e2ee543c258e519489659c99fb7f	A-GOO-TENS-101022/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35995**		
Divide By Zero	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Conv2D` is given empty `input` and the `filter` and `padding` sizes are valid, the output is all-zeros. This causes division-by-zero floating point exceptions that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 611d80db29dd7b0cfb755772c69d60ae5bca05f9. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/611d80db29dd7b0cfb755772c69d60ae5bca05f9, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q5jv-m6qw-5g37	A-GOO-TENS-101022/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35996		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `tf.sparse.cross` receives an input `separator` that is not a scalar, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 83dcb4dbfa094e33db084e97c4d0531a559e0ebf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35997**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p7hr-f446-x6qf, https://github.com/tensorflow/tensorflow/commit/83dcb4dbfa094e33db084e97c4d0531a559e0ebf	A-GOO-TENS-101022/483
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `EmptyTensorList`	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qhw4-wwr7-gjc5,	A-GOO-TENS-101022/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receives an input `element_shape` with more than one dimension, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c8ba76d48567aed347508e0552a257641931024d. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35998**	https://github.com/tensorflow/tensorflow/commit/c8ba76d48567aed347508e0552a257641931024d	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Conv2DBackpropInput` receives empty `out_backprop` inputs (e.g. `[3, 1, 0, 1]`), the current CPU/GPU kernels	https://github.com/tensorflow/tensorflow/commit/27a65a43cf763897fecfa5cdb5cc653fc5dd0346, https://github.com/tensorflow/tensorflow/security/advisories	A-GOO-TENS-101022/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`CHECK` fail (one with dnnl, the other with cudnn). This can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 27a65a43cf763897fecfa5cdb5cc653fc5dd0346. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35999**	/GHSA-37jf-mjv6-xfqw	
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqxc-pvf8-2w9v, https://github.com/tensorflow/tensorflow/commit/aed36912609fc07229b4d0a7b44f3f48efc00fd0	A-GOO-TENS-101022/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit aed36912609fc07229b4d0a7b44f3f48efc00fd0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36000**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `DrawBoundingBoxes` receives an input `boxes` that is not of dtype `float`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit da0d65cdc1270038e72157ba35bf74b85d9bda11. The fix will be included in TensorFlow 2.10.0. We will also	https://github.com/tensorflow/tensorflow/commit/da0d65cdc1270038e72157ba35bf74b85d9bda11, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jqm7-m5q7-3hm5	A-GOO-TENS-101022/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36001**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Unbatch` receives a nonscalar input `id`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 4419d10d576adefa36b0e0a9425d2569f7c0189f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mh3m-62v7-68xg, https://github.com/tensorflow/tensorflow/commit/4419d10d576adefa36b0e0a9425d2569f7c0189f	A-GOO-TENS-101022/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2022-36002**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RandomPoissonV2` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36003**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cv2p-32v3-vhwq, https://github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3	A-GOO-TENS-101022/489
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for	https://github.com/tensorflow/tensorflow/com	A-GOO-TENS-101022/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine learning. When `tf.random.gamma` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36004**	mit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv8m-8x97-937q	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_gradient` receives input `min` or `max` that is nonscalar, it	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-r26c-679w-mrjm, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15	A-GOO-TENS-101022/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36005**	e485e192bb319feed	
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit 1cf45b831eeb0cab8655c9c7c5d06ec6	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fv43-93gv-vm8f, https://github.com/tensorflow/tensorflow/commit/1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b	A-GOO-TENS-101022/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f45fc41b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36011**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it crashes. We have patched the issue in GitHub commit ad069af92392efee1418c48ff561fd3070a03d7b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jvhc-5hhr-w3v5, https://github.com/tensorflow/tensorflow/commit/ad069af92392efee1418c48ff561fd3070a03d7b	A-GOO-TENS-101022/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36012**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::GraphDefImporter::ConvertNodeDef` tries to convert NodeDefs without an op name, it crashes. We have patched the issue in GitHub commit a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36013**	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-828c-5j5q-vrjq	A-GOO-TENS-101022/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::TFOp::nameAttr` receives null type list attributes, it crashes. We have patched the issue in GitHub commits 3a754740d5414e362512ee981eefba41561a63a6 and a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36014**	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7j3m-8g3c-9qqq	A-GOO-TENS-101022/495
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RangeSize` receives values that do not fit into an `int64_t`, it	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rh87-q4vg-m45j, https://github.com/tensorflow/	A-GOO-TENS-101022/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crashes. We have patched the issue in GitHub commit 37e64539cd29fcfb814c4451152a60f5d107b0f0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36015**	tensorflow/commit/37e64539cd29fcfb814c4451152a60f5d107b0f0	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tensorflow::full_type::SubstituteFromAttrs` receives a `FullTypeDef& t` that is not exactly three args, it triggers a `CHECK`-fail instead of returning a status. We have patched the issue in GitHub commit 6104f0d4091c260ce9352f9155f7e9b725eab012. The fix	https://github.com/tensorflow/tensorflow/commit/6104f0d4091c260ce9352f9155f7e9b725eab012, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g468-qj8g-vcjc	A-GOO-TENS-101022/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36016**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Requantize` is given `input_min`, `input_max`, `requested_output_min`, `requested_output_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wqmc-pm8c-2jhc	A-GOO-TENS-101022/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36017**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedTensorToVariant` is given a `rt_nested_splits` list that contains tensors of ranks other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 88f93dfe691563baa4ae1e80ccde2d5c7a143821. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow	https://github.com/tensorflow/tensorflow/commit/88f93dfe691563baa4ae1e80ccde2d5c7a143821, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6cv-4fmf-66xf	A-GOO-TENS-101022/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36018**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVarsPerChannel` is given `min` or `max` tensors of a rank other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9j4v-pp28-mxv7	A-GOO-TENS-101022/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-36019**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizeAndDequantizeV3` is given a nonscalar `num_bits` input tensor, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit f3f9cb38ecfe5a8a703f2c4a8fead434ef291713. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36026**	https://github.com/tensorflow/tensorflow/commit/f3f9cb38ecfe5a8a703f2c4a8fead434ef291713, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9cr2-8pwr-fhfq	A-GOO-TENS-101022/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When converting transposed convolutions using per-channel weight quantization the converter segfaults and crashes the Python process. We have patched the issue in GitHub commit aa0b852a4588cea4d36b74feb05d93055540b450. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36027**	https://github.com/tensorflow/tensorflow/commit/aa0b852a4588cea4d36b74feb05d93055540b450, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-79h2-q768-fpxr	A-GOO-TENS-101022/502
Affected Version(s): 2.8.0					
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPool3DGradOp	https://github.com/tensorflow/tensorflow/commit/9178ac9d6389bdc54638ab913ea0e419234d14eb,	A-GOO-TENS-101022/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			` does not fully validate the input `orig_input_shape`. This results in an overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 9178ac9d6389bdc54638ab913ea0e419234d14eb. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35959**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wxjj-cgcx-r3vq	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. In `core/kernels/list_kernels.cc's TensorListReserve` , `num_elements` is assumed to be a	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v5xg-3q2c-c2r4, https://github.com/tensorflow/tensorflow/commit/b5f6fbfba7	A-GOO-TENS-101022/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tensor of size 1. When a `num_elements` of more than 1 element is provided, then `tf.raw_ops.TensorListReserve` fails the `CHECK_EQ` in `CheckIsAlignedAndSingleElement`. We have patched the issue in GitHub commit b5f6fbfba76576202b72119897561e3bd4f179c7. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35960**	6576202b72119897561e3bd4f179c7	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `FractionalAvgPoolGrad` does not fully validate the input	https://github.com/tensorflow/tensorflow/commit/03a659d7be9a1154fdf5eeac221e5950fec07dad, https://github.com/tensorflow/	A-GOO-TENS-101022/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`orig_input_tensor_shape`. This results in an overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 03a659d7be9a1154fdf5eeac221e5950fec07dad. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35963**	tensorflow/security/advisories/GHSA-84jm-4cf3-9jfm	
Affected Version(s): 2.9.0					
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPool3DGradOp` does not fully validate the input `orig_input_shape`. This results in an	https://github.com/tensorflow/tensorflow/commit/9178ac9d6389bdc54638ab913ea0e419234d14eb, https://github.com/tensorflow/tensorflow/security/advisories	A-GOO-TENS-101022/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 9178ac9d6389bdc54638ab913ea0e419234d14eb. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35959**	/GHSA-wxjj-cgcx-r3vq	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. In `core/kernels/list_kernels.cc's TensorListReserve`, `num_elements` is assumed to be a tensor of size 1. When a `num_elements` of more than 1	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v5xg-3q2c-c2r4, https://github.com/tensorflow/tensorflow/commit/b5f6fbfba76576202b72119897561e3bd4f179c7	A-GOO-TENS-101022/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			element is provided, then `tf.raw_ops.TensorListReserve` fails the `CHECK_EQ` in `CheckIsAlignedAndSingleElement`. We have patched the issue in GitHub commit b5f6fbfba76576202b72119897561e3bd4f179c7. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35960**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `FractionalAvgPoolGrad` does not fully validate the input `orig_input_tensor_shape`. This results in an overflow that results in a	https://github.com/tensorflow/tensorflow/commit/03a659d7be9a1154fdf5eeac221e5950fec07dad, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-84jm-4cf3-9jfm	A-GOO-TENS-101022/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 03a659d7be9a1154fdf5eeac221e5950fec07dad. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35963**		
Affected Version(s): From (including) 2.7.0 Up to (excluding) 2.7.2					
Out-of-bounds Write	16-Sep-2022	9.8	TensorFlow is an open source platform for machine learning. The `ScatterNd` function takes an input argument that determines the indices of of the output tensor. An input index greater than the output tensor or less than zero will either write content at	https://github.com/tensorflow/tensorflow/commit/b4d4b4cb019bd7240a52daa4ba61e3cc814f0384, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-ffjm-4qwc-7cmf	A-GOO-TENS-101022/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the wrong index or trigger a crash. We have patched the issue in GitHub commit b4d4b4cb019bd7240a52daa4ba61e3cc814f0384. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35939**		
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read is triggered. This issue has been patched in GitHub	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pxrw-j2fv-hx3h, https://github.com/tensorflow/tensorflow/commit/595a65a3e224a0362d7e68c2213acfc2b499a196	A-GOO-TENS-101022/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit 595a65a3e224a0362d7e68c2213acfc2b499a196. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35937**		
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. This issue has been patched in GitHub commit 4142e47e9e31db481781b955ed3ff80	https://github.com/tensorflow/tflite-micro/commit/4142e47e9e31db481781b955ed3ff807a781b494, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-3m3g-pf5v-5hpj	A-GOO-TENS-101022/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7a781b494. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35938**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of tf.reshape op in TensorFlow is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by overflowing the number of elements in a tensor. This issue has been patched in GitHub commit 61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555. The fix will be included in TensorFlow 2.10.0. We will also	https://github.com/tensorflow/tensorflow/commit/61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f4w6-h4f5-wx45	A-GOO-TENS-101022/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35934**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of SobolSampleOp is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by assuming `input(0)`, `input(1)`, and `input(2)` to be scalar. This issue has been patched in GitHub commit c65c67f88ad770662e8f191269a907bf2b94b1bf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-97p7-w86h-vcf9, https://github.com/tensorflow/tensorflow/commit/c65c67f88ad770662e8f191269a907bf2b94b1bf	A-GOO-TENS-101022/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35935**		
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `RaggedRangOp` function takes an argument `limits` that is eventually used to construct a `TensorShape` as an `int64`. If `limits` is a very large float, it can overflow when converted to an `int64`. This triggers an `InvalidArgument` but also throws an abort signal that crashes the program. We have patched the issue in GitHub commit 37cefa91bee4eace55715eeef43720b958a01192. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-x989-q2pq-4q5x, https://github.com/tensorflow/tensorflow/commit/37cefa91bee4eace55715eeef43720b958a01192	A-GOO-TENS-101022/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35940**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `AvgPoolOp` function takes an argument `ksize` that must be positive but is not checked. A negative `ksize` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mgmh-g2v6-mqw5	A-GOO-TENS-101022/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds to this issue. **CVE ID : CVE-2022-35941**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `UnbatchGradOp` function takes an argument `id` that is assumed to be a scalar. A nonscalar `id` can trigger a `CHECK` failure and crash the program. It also requires its argument `batch_index` to contain three times the number of elements as indicated in its `batch_index.dim_size(0)`. An incorrect `batch_index` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 5f945fc6409a3c1e90d6970c9292f805f6e6ddf2. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on	https://github.com/tensorflow/tensorflow/commit/5f945fc6409a3c1e90d6970c9292f805f6e6ddf2, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h5vq-gw2c-pq47	A-GOO-TENS-101022/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35952**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPool3DGradOp` does not fully validate the input `orig_input_shape`. This results in an overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 9178ac9d6389bdc54638ab913ea0e419234d14eb. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow	https://github.com/tensorflow/tensorflow/commit/9178ac9d6389bdc54638ab913ea0e419234d14eb, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wxjj-cgcx-r3vq	A-GOO-TENS-101022/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35959**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. In `core/kernels/list_kernels.cc's TensorListReserve`, `num_elements` is assumed to be a tensor of size 1. When a `num_elements` of more than 1 element is provided, then `tf.raw_ops.TensorListReserve` fails the `CHECK_EQ` in `CheckIsAlignedAndSingleElement`. We have patched the issue in GitHub commit b5f6fbfba76576202b72119897561e3bd4f179c7. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v5xg-3q2c-c2r4, https://github.com/tensorflow/tensorflow/commit/b5f6fbfba76576202b72119897561e3bd4f179c7	A-GOO-TENS-101022/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35960**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `FractionalAvgPoolGrad` does not fully validate the input `orig_input_tensor_shape`. This results in an overflow that results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 03a659d7be9a1154fdf5eeac221e5950fec07dad. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and	https://github.com/tensorflow/tensorflow/commit/03a659d7be9a1154fdf5eeac221e5950fec07dad, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-84jm-4cf3-9jfm	A-GOO-TENS-101022/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35963**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `BlockLSTMGradV2` does not fully validate its inputs. This results in a a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 2a458fc4866505be27c62f81474ecb2b870498fa. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35964**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f7r5-q7cx-h668, https://github.com/tensorflow/tensorflow/commit/2a458fc4866505be27c62f81474ecb2b870498fa	A-GOO-TENS-101022/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LowerBound` or `UpperBound` is given an empty`sorted_inputs` input, it results in a `nullptr` dereference, leading to a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bce3717eaef4f769019fd18e990464ca4a2efeea. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35965**	https://github.com/tensorflow/tensorflow/commit/bce3717eaef4f769019fd18e990464ca4a2efeea, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qxpx-j395-pw36	A-GOO-TENS-101022/521
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If	https://github.com/tensorflow/tensorflow/commit/7cdf9d4d2083b739ec81cf	A-GOO-TENS-101022/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`QuantizedAvgPool` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7cdf9d4d2083b739ec81cfdace546b0c99f50622. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35966**	dace546b0c99f50622, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4w68-4x85-mjj9	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedAdd` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v6h3-348g-6h5x, https://github.com/tensorflow/tensorflow/commit/49b3824d8	A-GOO-TENS-101022/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35967**	3af706df0ad07e4e677d88659756d89	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPoolGrad` does not fully validate the input `orig_input_shape`. This results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-2475-53vw-vp25	A-GOO-TENS-101022/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35968**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `Conv2DBackpropInput` requires `input_sizes` to be 4-dimensional. Otherwise, it gives a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 50156d547b9a1da0144d7babe665cf690305b33c. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/50156d547b9a1da0144d7babe665cf690305b33c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q2c3-jpmc-gfjx	A-GOO-TENS-101022/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35969**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedInstanceNorm` is given `x_min` or `x_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g35r-369w-3fqp	A-GOO-TENS-101022/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35970**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVars` is given `min` or `max` tensors of a nonzero rank, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9fpg-838v-wpv7	A-GOO-TENS-101022/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2022-35971**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedBiasAdd` is given `min_input`, `max_input`, `min_bias`, `max_bias` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4pc4-m9mj-v2r9	A-GOO-TENS-101022/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35972		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedMatMul` is given nonscalar input for: `min_a`, `max_a`, `min_b`, or `max_b` It gives a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit aca766ac7693bf29ed0df55ad6bfcc78f35e7f48. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35973**	https://github.com/tensorflow/tensorflow/commit/aca766ac7693bf29ed0df55ad6bfcc78f35e7f48, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-689c-r7h2-fv9v	A-GOO-TENS-101022/529
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vgvh-	A-GOO-TENS-101022/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`QuantizeDownAndShrinkRange` is given nonscalar inputs for `input_min` or `input_max`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 73ad1815ebcfeb7c051f9c2f7ab5024380ca8613. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35974**	2pf4-jr2x, https://github.com/tensorflow/tensorflow/commit/73ad1815ebcfeb7c051f9c2f7ab5024380ca8613	
Affected Version(s): From (including) 2.8.0 Up to (excluding) 2.8.1					
Out-of-bounds Write	16-Sep-2022	9.8	TensorFlow is an open source platform for machine learning. The `ScatterNd` function takes an input argument that determines the indices of of the	https://github.com/tensorflow/tensorflow/commit/b4d4b4cb019bd7240a52daa4ba61e3cc814f0384, https://github.com/tensorflow/	A-GOO-TENS-101022/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			output tensor. An input index greater than the output tensor or less than zero will either write content at the wrong index or trigger a crash. We have patched the issue in GitHub commit b4d4b4cb019bd7240a52daa4ba61e3cc814f0384. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35939**	tensorflow/security/advisories/GHSA-ffjm-4qwc-7cmf	
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or	https://github.com/tensorflow/tflite-micro/commit/4142e47e9e31db481781b955ed3ff807a781b494, https://github.com/tensorflow/tensorflow/security/advisories	A-GOO-TENS-101022/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. This issue has been patched in GitHub commit 4142e47e9e31db481781b955ed3ff807a781b494. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35938**	/GHSA-3m3g-pf5v-5hpj	
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pxrw-j2fv-hx3h, https://github.com/tensorflow/tensorflow/commit/595a65a3e224a0362d7e68c2213acfc2b499a196	A-GOO-TENS-101022/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read is triggered. This issue has been patched in GitHub commit 595a65a3e224a0362d7e68c2213acfc2b499a196. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35937**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of tf.reshape op in TensorFlow is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by overflowing the number of elements in a tensor. This issue has been patched in GitHub commit	https://github.com/tensorflow/tensorflow/commit/61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f4w6-h4f5-wx45	A-GOO-TENS-101022/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35934**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of SobolSampleOp is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by assuming `input(0)`, `input(1)`, and `input(2)` to be scalar. This issue has been patched in GitHub commit c65c67f88ad770662e8f191269a907bf2b94b1bf. The fix will be included in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-97p7-w86h-vcf9, https://github.com/tensorflow/tensorflow/commit/c65c67f88ad770662e8f191269a907bf2b94b1bf	A-GOO-TENS-101022/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35935**		
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `RaggedRangOp` function takes an argument `limits` that is eventually used to construct a `TensorShape` as an `int64`. If `limits` is a very large float, it can overflow when converted to an `int64`. This triggers an `InvalidArgument` but also throws an abort signal that crashes the program. We have patched the issue in GitHub commit 37cefa91bee4eace55715eeef43720b958a01192. The fix	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-x989-q2pq-4q5x, https://github.com/tensorflow/tensorflow/commit/37cefa91bee4eace55715eeef43720b958a01192	A-GOO-TENS-101022/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35940**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `AvgPoolOp` function takes an argument `ksize` that must be positive but is not checked. A negative `ksize` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mgmh-g2v6-mqw5	A-GOO-TENS-101022/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds to this issue. **CVE ID : CVE-2022-35941**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `UnbatchGradOp` function takes an argument `id` that is assumed to be a scalar. A nonscalar `id` can trigger a `CHECK` failure and crash the program. It also requires its argument `batch_index` to contain three times the number of elements as indicated in its `batch_index.dim_size(0)`. An incorrect `batch_index` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 5f945fc6409a3c1e90d6970c9292f80	https://github.com/tensorflow/tensorflow/commit/5f945fc6409a3c1e90d6970c9292f805f6e6ddf2, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h5vq-gw2c-pq47	A-GOO-TENS-101022/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5f6e6ddf2. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35952**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `BlockLSTMGradV2` does not fully validate its inputs. This results in a a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 2a458fc4866505be27c62f81474ecb2b870498fa. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f7r5-q7cx-h668, https://github.com/tensorflow/tensorflow/commit/2a458fc4866505be27c62f81474ecb2b870498fa	A-GOO-TENS-101022/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35964**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LowerBound` or `UpperBound` is given an empty`sorted_inputs` input, it results in a `nullptr` dereference, leading to a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bce3717eaef4f769019fd18e990464ca4a2efeea. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/commit/bce3717eaef4f769019fd18e990464ca4a2efeea, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qxpx-j395-pw36	A-GOO-TENS-101022/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35965**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedAvgPool` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7cdf9d4d2083b739ec81cfdace546b0c99f50622. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/7cdf9d4d2083b739ec81cfdace546b0c99f50622, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4w68-4x85-mjj9	A-GOO-TENS-101022/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35966		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedAdd` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35967**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v6h3-348g-6h5x, https://github.com/tensorflow/tensorflow/commit/49b3824d83af706df0ad07e4e677d88659756d89	A-GOO-TENS-101022/542
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b11	A-GOO-TENS-101022/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implementation of `AvgPoolGrad` does not fully validate the input `orig_input_shape`. This results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35968**	4e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-2475-53vw-vp25	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `Conv2DBackpropInput` requires `input_sizes` to be 4-dimensional.	https://github.com/tensorflow/tensorflow/commit/50156d547b9a1da0144d7babe665cf690305b33c, https://github.com/tensorflow/tensorflow/sec	A-GOO-TENS-101022/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Otherwise, it gives a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 50156d547b9a1da0144d7babe665cf690305b33c. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35969**	urity/advisories/GHSA-q2c3-jpmc-gfjx	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedInstanceNorm` is given `x_min` or `x_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g35r-369w-3fqp	A-GOO-TENS-101022/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35970**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVars` is given `min` or `max` tensors of a nonzero rank, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9fpg-838v-wpv7	A-GOO-TENS-101022/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35971**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedBiasAdd` is given `min_input`, `max_input`, `min_bias`, `max_bias` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4pc4-m9mj-v2r9	A-GOO-TENS-101022/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35972**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedMatMul` is given nonscalar input for: `min_a`, `max_a`, `min_b`, or `max_b` It gives a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit aca766ac7693bf29ed0df55ad6bfcc78f35e7f48. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/commit/aca766ac7693bf29ed0df55ad6bfcc78f35e7f48, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-689c-r7h2-fv9v	A-GOO-TENS-101022/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35973**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizeDownAndShrinkRange` is given nonscalar inputs for `input_min` or `input_max`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 73ad1815ebcfeb7c051f9c2f7ab5024380ca8613. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vgvh-2pf4-jr2x, https://github.com/tensorflow/tensorflow/commit/73ad1815ebcfeb7c051f9c2f7ab5024380ca8613	A-GOO-TENS-101022/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35974		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedRelu` or `QuantizedRelu6` are given nonscalar inputs for `min_features` or `max_features`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35979**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v7vw-577f-vp8x, https://github.com/tensorflow/tensorflow/commit/49b3824d83af706df0ad07e4e677d88659756d89	A-GOO-TENS-101022/550
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for	https://github.com/tensorflow/tensorflow/com	A-GOO-TENS-101022/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine learning. `FractionalMaxPoolGrad` validates its inputs with `CHECK` failures instead of with returning errors. If it gets incorrectly sized inputs, the `CHECK` failure can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 8741e57d163a079db05a7107a7609af70931def4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35981**	mit/8741e57d163a079db05a7107a7609af70931def4, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vxv8-r8q2-63xw	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `SparseBincount` is given inputs for `indices`, `values`, and `dense_shape`	https://github.com/tensorflow/tensorflow/commit/40adbe4dd15b582b0210dfbf40c243a62f5119fa, https://github.c	A-GOO-TENS-101022/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that do not make a valid sparse tensor, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 40adbe4dd15b582b0210dfbf40c243a62f5119fa. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35982**	om/tensorflow/tensorflow/security/advisories/GHSA-397c-5g2j-qxpv	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Save` or `SaveSlices` is run over tensors of an unsupported `dtype`, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6vp-8q9j-whx4, https://github.com/tensorflow/tensorflow/commit/5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4	A-GOO-TENS-101022/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue in GitHub commit 5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35983**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `ParameterizedTruncatedNormal` assumes `shape` is of type `int32`. A valid `shape` of type `int64` results in a mismatched type `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 72180be03447a10810edca700cbc9af690dfeb51. The fix	https://github.com/tensorflow/tensorflow/commit/72180be03447a10810edca700cbc9af690dfeb51, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p2xf-8hgm-hpw5	A-GOO-TENS-101022/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35984**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LRNGrad` is given an `output_image` input tensor that is not 4-D, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bd90b3efab4ec958b228cd7cfe9125be1c0cf255. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9942-r22v-78cp, https://github.com/tensorflow/tensorflow/commit/bd90b3efab4ec958b228cd7cfe9125be1c0cf255	A-GOO-TENS-101022/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35985**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedBincount` is given an empty input tensor `splits`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7a4591fd4f065f4fa903593bc39b2f79530a74b8. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/7a4591fd4f065f4fa903593bc39b2f79530a74b8, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wr9v-g9vf-c74v	A-GOO-TENS-101022/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35986		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `DenseBincount` assumes its input tensor `weights` to either have the same shape as its input tensor `input` or to be length-0. A different `weights` shape will trigger a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf4c14353c2328636a18bfad1e151052c81d5f43. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35987**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-w62h-8xjm-fv49, https://github.com/tensorflow/tensorflow/commit/bf4c14353c2328636a18bfad1e151052c81d5f43	A-GOO-TENS-101022/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.linalg.matrix_rank` receives an empty input `a`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35988**	https://github.com/tensorflow/tensorflow/commit/c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9vqj-64pv-w55c	A-GOO-TENS-101022/558
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `MaxPool` receives a window size input array	https://github.com/tensorflow/tensorflow/commit/32d7bd3defd134f21a4e344c8dfd40099aaf6b18,	A-GOO-TENS-101022/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`ksize` with dimensions greater than its input tensor `input`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 32d7bd3defd134f21a4e344c8dfd40099aaf6b18. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35989**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j43h-pgmg-5hjq	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_per_channel_gradient` receives input `min` or `max` of	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h7ff-cfc9-wmmh, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15	A-GOO-TENS-101022/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rank other than 1, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range.There are no known workarounds for this issue. **CVE ID : CVE-2022-35990**	e485e192bb319feed	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListScatter` and `TensorListScatterV2` receive an `element_shape` of a rank greater than one, they give a `CHECK` fail that can trigger a denial of service attack. We have patched	https://github.com/tensorflow/tensorflow/commit/bb03fdf4aae944ab2e4b35c7daa051068a8b7f61, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vm7x-4qhj-rrcq	A-GOO-TENS-101022/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue in GitHub commit bb03fdf4aae944ab2e4b35c7daa051068a8b7f61. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35991**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListFromTensor` receives an `element_shape` of a rank greater than one, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 3db59a042a38f4338aa207922fa2f476e000a6ee. The fix will be included in TensorFlow 2.10.0.	https://github.com/tensorflow/tensorflow/commit/3db59a042a38f4338aa207922fa2f476e000a6ee, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9v8w-xmr4-wgxp	A-GOO-TENS-101022/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35992**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `SetSize` receives an input `set_shape` that is not a 1D tensor, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit cf70b79d2662c0d3c6af74583641e345fc939467. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and	https://github.com/tensorflow/tensorflow/commit/cf70b79d2662c0d3c6af74583641e345fc939467, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wq6q-6m32-9rv9	A-GOO-TENS-101022/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35993**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `CollectiveGather` receives an scalar input `input`, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c1f491817dec39a26be3c574e86a88c30f3c4770. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35994**	https://github.com/tensorflow/tensorflow/commit/c1f491817dec39a26be3c574e86a88c30f3c4770, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fhfc-2q7x-929f	A-GOO-TENS-101022/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `AudioSummaryV2` receives an input `sample_rate` with more than one element, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf6b45244992e2ee543c258e519489659c99fb7f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35995**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9h5-vr8m-x2h4, https://github.com/tensorflow/tensorflow/commit/bf6b45244992e2ee543c258e519489659c99fb7f	A-GOO-TENS-101022/565
Divide By Zero	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Conv2D` is given empty `input` and	https://github.com/tensorflow/tensorflow/commit/611d80db29dd7b0cfb755772c69d60ae5bc	A-GOO-TENS-101022/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the `filter` and `padding` sizes are valid, the output is all-zeros. This causes division-by-zero floating point exceptions that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 611d80db29dd7b0cfb755772c69d60ae5bca05f9. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35996**	a05f9, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q5jv-m6qw-5g37	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `tf.sparse.cross` receives an input `separator` that is not a scalar, it gives a `CHECK` fail that can be used to trigger a denial of	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p7hr-f446-x6qf, https://github.com/tensorflow/tensorflow/commit/83dcb4dbfa094e33db084e	A-GOO-TENS-101022/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service attack. We have patched the issue in GitHub commit 83dcb4dbfa094e33db084e97c4d0531a559e0ebf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35997**	97c4d0531a559e0ebf	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `EmptyTensorList` receives an input `element_shape` with more than one dimension, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c8ba76d48567aed347508e0552a257	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qhw4-wwr7-gjc5, https://github.com/tensorflow/tensorflow/commit/c8ba76d48567aed347508e0552a257641931024d	A-GOO-TENS-101022/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			641931024d. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35998**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Conv2DBackpropInput` receives empty `out_backprop` inputs (e.g. `[3, 1, 0, 1]`), the current CPU/GPU kernels `CHECK` fail (one with dnnl, the other with cudnn). This can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 27a65a43cf763897fecfa5cdb5cc653fc5dd0346. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/27a65a43cf763897fecfa5cdb5cc653fc5dd0346, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-37jf-mjv6-xfqw	A-GOO-TENS-101022/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35999**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit aed36912609fc07229b4d0a7b44f3f48efc00fd0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqxc-pvf8-2w9v, https://github.com/tensorflow/tensorflow/commit/aed36912609fc07229b4d0a7b44f3f48efc00fd0	A-GOO-TENS-101022/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36000**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `DrawBoundingBoxes` receives an input `boxes` that is not of dtype `float`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit da0d65cdc1270038e72157ba35bf74b85d9bda11. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/da0d65cdc1270038e72157ba35bf74b85d9bda11, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jqm7-m5q7-3hm5	A-GOO-TENS-101022/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36001		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Unbatch` receives a nonscalar input `id`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 4419d10d576adefa36b0e0a9425d2569f7c0189f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36002**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mh3m-62v7-68xg, https://github.com/tensorflow/tensorflow/commit/4419d10d576adefa36b0e0a9425d2569f7c0189f	A-GOO-TENS-101022/572
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RandomPoissonV2` receives large	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cv2p-32v3-vhwq, https://github.c	A-GOO-TENS-101022/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36003**	om/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.random.gamma` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv8m-8x97-937q	A-GOO-TENS-101022/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36004**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_gradient` receives input `min` or `max` that is nonscalar, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-r26c-679w-mrjm, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319feed	A-GOO-TENS-101022/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36005**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit 1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fv43-93gv-vm8f, https://github.com/tensorflow/tensorflow/commit/1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b	A-GOO-TENS-101022/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36011**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it crashes. We have patched the issue in GitHub commit ad069af92392efee1418c48ff561fd3070a03d7b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36012**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jvhc-5hhr-w3v5, https://github.com/tensorflow/tensorflow/commit/ad069af92392efee1418c48ff561fd3070a03d7b	A-GOO-TENS-101022/577
NULL Pointer	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning.	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c	A-GOO-TENS-101022/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			When `mlir::tfg::GraphDefImporter::ConvertNodeDef` tries to convert NodeDefs without an op name, it crashes. We have patched the issue in GitHub commit a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36013**	9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-828c-5j5q-vrjq	
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::TFOp::nameAttr` receives null type list attributes, it crashes. We have patched the issue in GitHub commits 3a754740d5414e3	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7j3m-8g3c-9qqq	A-GOO-TENS-101022/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			62512ee981eefba41561a63a6 and a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36014**		
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RangeSize` receives values that do not fit into an `int64_t`, it crashes. We have patched the issue in GitHub commit 37e64539cd29fcfb814c4451152a60f5d107b0f0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rh87-q4vg-m45j, https://github.com/tensorflow/tensorflow/commit/37e64539cd29fcfb814c4451152a60f5d107b0f0	A-GOO-TENS-101022/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36015**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tensorflow::full_type::SubstituteFromAttrs` receives a `FullTypeDef& t` that is not exactly three args, it triggers a `CHECK`-fail instead of returning a status. We have patched the issue in GitHub commit 6104f0d4091c260ce9352f9155f7e9b725eab012. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/6104f0d4091c260ce9352f9155f7e9b725eab012, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g468-qj8g-vcjc	A-GOO-TENS-101022/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-36016**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Requantize` is given `input_min`, `input_max`, `requested_output_min`, `requested_output_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36017**	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wqmc-pm8c-2jhc	A-GOO-TENS-101022/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedTensorToVariant` is given a `rt_nested_splits` list that contains tensors of ranks other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 88f93dfe691563baa4ae1e80ccde2d5c7a143821. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36018**	https://github.com/tensorflow/tensorflow/commit/88f93dfe691563baa4ae1e80ccde2d5c7a143821, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6cv-4fmf-66xf	A-GOO-TENS-101022/583
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning.	https://github.com/tensorflow/tensorflow/commit/785d67a78	A-GOO-TENS-101022/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			If `FakeQuantWithMinMaxVarsPerChannel` is given `min` or `max` tensors of a rank other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36019**	a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9j4v-pp28-mxv7	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizeAndDequantizeV3` is given a nonscalar `num_bits` input	https://github.com/tensorflow/tensorflow/commit/f3f9cb38ecfe5a8a703f2c4a8fead434ef291713, https://github.com/tensorflow/	A-GOO-TENS-101022/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tensor, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit f3f9cb38ecfe5a8a703f2c4a8fead434ef291713. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36026**	tensorflow/security/advisories/GHSA-9cr2-8pwr-fhfq	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When converting transposed convolutions using per-channel weight quantization the converter segfaults and crashes the Python process. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/aa0b852a4588cea4d36b74feb05d93055540b450, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-79h2-q768-fpxr	A-GOO-TENS-101022/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aa0b852a4588cea4d36b74feb05d93055540b450. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36027**		
Affected Version(s): From (including) 2.9.0 Up to (excluding) 2.9.1					
Out-of-bounds Write	16-Sep-2022	9.8	TensorFlow is an open source platform for machine learning. The `ScatterNd` function takes an input argument that determines the indices of of the output tensor. An input index greater than the output tensor or less than zero will either write content at the wrong index or trigger a crash. We have patched the issue in GitHub commit b4d4b4cb019bd7240a52daa4ba61e3	https://github.com/tensorflow/tensorflow/commit/b4d4b4cb019bd7240a52daa4ba61e3cc814f0384, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-ffjm-4qwc-7cmf	A-GOO-TENS-101022/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cc814f0384. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35939**		
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. This issue has been patched in GitHub commit 4142e47e9e31db481781b955ed3ff807a781b494. The fix will be included in TensorFlow 2.10.0.	https://github.com/tensorflow/tflite-micro/commit/4142e47e9e31db481781b955ed3ff807a781b494, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-3m3g-pf5v-5hpj	A-GOO-TENS-101022/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35938**		
Out-of-bounds Read	16-Sep-2022	9.1	TensorFlow is an open source platform for machine learning. The `GatherNd` function takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read is triggered. This issue has been patched in GitHub commit 595a65a3e224a0362d7e68c2213acfc2b499a196. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-pxrw-j2fv-hx3h, https://github.com/tensorflow/tensorflow/commit/595a65a3e224a0362d7e68c2213acfc2b499a196	A-GOO-TENS-101022/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35937**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of tf.reshape op in TensorFlow is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by overflowing the number of elements in a tensor. This issue has been patched in GitHub commit 61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and	https://github.com/tensorflow/tensorflow/commit/61f0f9b94df8c0411f0ad0ecc2fec2d3f3c33555, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f4w6-h4f5-wx45	A-GOO-TENS-101022/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35934**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of SobolSampleOp is vulnerable to a denial of service via CHECK-failure (assertion failure) caused by assuming `input(0)`, `input(1)`, and `input(2)` to be scalar. This issue has been patched in GitHub commit c65c67f88ad770662e8f191269a907bf2b94b1bf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-97p7-w86h-vcf9, https://github.com/tensorflow/tensorflow/commit/c65c67f88ad770662e8f191269a907bf2b94b1bf	A-GOO-TENS-101022/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-35935**		
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `RaggedRangOp` function takes an argument `limits` that is eventually used to construct a `TensorShape` as an `int64`. If `limits` is a very large float, it can overflow when converted to an `int64`. This triggers an `InvalidArgument` but also throws an abort signal that crashes the program. We have patched the issue in GitHub commit 37cefa91bee4eace55715eeef43720b958a01192. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-x989-q2pq-4q5x, https://github.com/tensorflow/tensorflow/commit/37cefa91bee4eace55715eeef43720b958a01192	A-GOO-TENS-101022/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2022-35940**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `AvgPoolOp` function takes an argument `ksize` that must be positive but is not checked. A negative `ksize` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds to this issue. **CVE ID : CVE-2022-35941**	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mgmh-g2v6-mqw5	A-GOO-TENS-101022/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The `UnbatchGradOp` function takes an argument `id` that is assumed to be a scalar. A nonscalar `id` can trigger a `CHECK` failure and crash the program. It also requires its argument `batch_index` to contain three times the number of elements as indicated in its `batch_index.dim_size(0)`. An incorrect `batch_index` can trigger a `CHECK` failure and crash the program. We have patched the issue in GitHub commit 5f945fc6409a3c1e90d6970c9292f805f6e6ddf2. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/commit/5f945fc6409a3c1e90d6970c9292f805f6e6ddf2, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h5vq-gw2c-pq47	A-GOO-TENS-101022/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35952**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `BlockLSTMGradV2` does not fully validate its inputs. This results in a a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 2a458fc4866505be27c62f81474ecb2b870498fa. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35964**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-f7r5-q7cx-h668, https://github.com/tensorflow/tensorflow/commit/2a458fc4866505be27c62f81474ecb2b870498fa	A-GOO-TENS-101022/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LowerBound` or `UpperBound` is given an empty`sorted_inputs` input, it results in a `nullptr` dereference, leading to a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bce3717eaef4f769019fd18e990464ca4a2efeea. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35965**	https://github.com/tensorflow/tensorflow/commit/bce3717eaef4f769019fd18e990464ca4a2efeea, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qxpx-j395-pw36	A-GOO-TENS-101022/596
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If	https://github.com/tensorflow/tensorflow/commit/7cdf9d4d2083b739ec81cf	A-GOO-TENS-101022/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`QuantizedAvgPool` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7cdf9d4d2083b739ec81cfdace546b0c99f50622. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35966**	dace546b0c99f50622, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4w68-4x85-mjj9	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedAdd` is given `min_input` or `max_input` tensors of a nonzero rank, it results in a segfault	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v6h3-348g-6h5x, https://github.com/tensorflow/tensorflow/commit/49b3824d8	A-GOO-TENS-101022/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35967**	3af706df0ad07e4e677d88659756d89	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `AvgPoolGrad` does not fully validate the input `orig_input_shape`. This results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub	https://github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-2475-53vw-vp25	A-GOO-TENS-101022/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35968**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. The implementation of `Conv2DBackpropInput` requires `input_sizes` to be 4-dimensional. Otherwise, it gives a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 50156d547b9a1da0144d7babe665cf690305b33c. The fix will be included in	https://github.com/tensorflow/tensorflow/commit/50156d547b9a1da0144d7babe665cf690305b33c, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q2c3-jpmc-gfjx	A-GOO-TENS-101022/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35969**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedInstanceNorm` is given `x_min` or `x_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g35r-369w-3fqp	A-GOO-TENS-101022/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35970**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVars` is given `min` or `max` tensors of a nonzero rank, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9fpg-838v-wpv7	A-GOO-TENS-101022/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2022-35971**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedBiasAdd` is given `min_input`, `max_input`, `min_bias`, `max_bias` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-4pc4-m9mj-v2r9	A-GOO-TENS-101022/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35972		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedMatMul` is given nonscalar input for: `min_a`, `max_a`, `min_b`, or `max_b` It gives a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit aca766ac7693bf29ed0df55ad6bfcc78f35e7f48. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35973**	https://github.com/tensorflow/tensorflow/commit/aca766ac7693bf29ed0df55ad6bfcc78f35e7f48, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-689c-r7h2-fv9v	A-GOO-TENS-101022/604
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vgvh-	A-GOO-TENS-101022/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`QuantizeDownAndShrinkRange` is given nonscalar inputs for `input_min` or `input_max`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 73ad1815ebcfeb7c051f9c2f7ab5024380ca8613. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35974**	2pf4-jr2x, https://github.com/tensorflow/tensorflow/commit/73ad1815ebcfeb7c051f9c2f7ab5024380ca8613	
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizedRelu` or `QuantizedRelu6` are given nonscalar inputs for `min_features` or	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-v7vw-577f-vp8x, https://github.com/tensorflow/tensorflow/commit/49b3824d8	A-GOO-TENS-101022/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`max_features`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 49b3824d83af706df0ad07e4e677d88659756d89. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35979**	3af706df0ad07e4e677d88659756d89	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `FractionalMaxPoolGrad` validates its inputs with `CHECK` failures instead of with returning errors. If it gets incorrectly sized inputs, the `CHECK` failure can be used to trigger a denial of service	https://github.com/tensorflow/tensorflow/commit/8741e57d163a079db05a7107a7609af70931def4, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vxv8-r8q2-63xw	A-GOO-TENS-101022/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack. We have patched the issue in GitHub commit 8741e57d163a079db05a7107a7609af70931def4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35981**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `SparseBincount` is given inputs for `indices`, `values`, and `dense_shape` that do not make a valid sparse tensor, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 40adbe4dd15b582b0210dfbf40c243a62f5119fa. The fix	https://github.com/tensorflow/tensorflow/commit/40adbe4dd15b582b0210dfbf40c243a62f5119fa, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-397c-5g2j-qxpv	A-GOO-TENS-101022/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35982**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Save` or `SaveSlices` is run over tensors of an unsupported `dtype`, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-m6vp-8q9j-whx4, https://github.com/tensorflow/tensorflow/commit/5dd7b86b84a864b834c6fa3d7f9f51c87efa99d4	A-GOO-TENS-101022/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35983**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `ParameterizedTruncatedNormal` assumes `shape` is of type `int32`. A valid `shape` of type `int64` results in a mismatched type `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 72180be03447a10810edca700cbc9af690dfeb51. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no	https://github.com/tensorflow/tensorflow/commit/72180be03447a10810edca700cbc9af690dfeb51, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p2xf-8hgm-hpw5	A-GOO-TENS-101022/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this issue. **CVE ID : CVE-2022-35984**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `LRNGrad` is given an `output_image` input tensor that is not 4-D, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bd90b3efab4ec958b228cd7cfe9125be1c0cf255. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35985**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9942-r22v-78cp, https://github.com/tensorflow/tensorflow/commit/bd90b3efab4ec958b228cd7cfe9125be1c0cf255	A-GOO-TENS-101022/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedBincount` is given an empty input tensor `splits`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 7a4591fd4f065f4fa903593bc39b2f79530a74b8. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35986**	https://github.com/tensorflow/tensorflow/commit/7a4591fd4f065f4fa903593bc39b2f79530a74b8, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wr9v-g9vf-c74v	A-GOO-TENS-101022/612
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. `DenseBincount` assumes its input tensor `weights` to either have the	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-w62h-8xjm-fv49, https://github.com/tensorflow/	A-GOO-TENS-101022/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			same shape as its input tensor `input` or to be length-0. A different `weights` shape will trigger a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit bf4c14353c2328636a18bfad1e1510 52c81d5f43. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35987**	tensorflow/commit/bf4c14353c2328636a18bfad1e151052c81d5f43	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.linalg.matrix_rank` receives an empty input `a`, the GPU kernel gives a `CHECK` fail that can be used to	https://github.com/tensorflow/tensorflow/commit/c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a, https://github.com/tensorflow/tensorflow/security/advisories	A-GOO-TENS-101022/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger a denial of service attack. We have patched the issue in GitHub commit c55b476aa0e0bd4ee99d0f3ad18d9d706cd1260a. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35988**	/GHSA-9vqj-64pv-w55c	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `MaxPool` receives a window size input array `ksize` with dimensions greater than its input tensor `input`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub	https://github.com/tensorflow/tensorflow/commit/32d7bd3defd134f21a4e344c8dfd40099aaf6b18, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-j43h-pgmg-5hjq	A-GOO-TENS-101022/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit 32d7bd3defd134f21a4e344c8dfd40099aaf6b18. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35989**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_per_channel_gradient` receives input `min` or `max` of rank other than 1, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-h7ff-cfc9-wmmh, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319feed	A-GOO-TENS-101022/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range.There are no known workarounds for this issue. **CVE ID : CVE-2022-35990**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListScatter` and `TensorListScatterV2` receive an `element_shape` of a rank greater than one, they give a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit bb03fdf4aae944ab2e4b35c7daa051068a8b7f61. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1,	https://github.com/tensorflow/tensorflow/commit/bb03fdf4aae944ab2e4b35c7daa051068a8b7f61, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-vm7x-4qhj-rrcq	A-GOO-TENS-101022/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35991**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `TensorListFromTensor` receives an `element_shape` of a rank greater than one, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 3db59a042a38f4338aa207922fa2f476e000a6ee. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/3db59a042a38f4338aa207922fa2f476e000a6ee, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9v8w-xmr4-wgxp	A-GOO-TENS-101022/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-35992**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `SetSize` receives an input `set_shape` that is not a 1D tensor, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit cf70b79d2662c0d3c6af74583641e345fc939467. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35993**	https://github.com/tensorflow/tensorflow/commit/cf70b79d2662c0d3c6af74583641e345fc939467, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wq6q-6m32-9rv9	A-GOO-TENS-101022/619
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning.	https://github.com/tensorflow/tensorflow/commit/c1f491817	A-GOO-TENS-101022/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When `CollectiveGather` receives an scalar input `input`, it gives a `CHECK` fails that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c1f491817dec39a26be3c574e86a88c30f3c4770. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35994**	dec39a26be3c574e86a88c30f3c4770, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fhfc-2q7x-929f	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `AudioSummaryV2` receives an input `sample_rate` with more than one element, it gives a `CHECK` fails that can be used to	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g9h5-vr8m-x2h4, https://github.com/tensorflow/tensorflow/commit/bf6b45244992e2ee543c25	A-GOO-TENS-101022/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger a denial of service attack. We have patched the issue in GitHub commit bf6b45244992e2ee543c258e519489659c99fb7f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35995**	8e519489659c99fb7f	
Divide By Zero	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Conv2D` is given empty `input` and the `filter` and `padding` sizes are valid, the output is all-zeros. This causes division-by-zero floating point exceptions that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit	https://github.com/tensorflow/tensorflow/commit/611d80db29dd7b0cfb755772c69d60ae5bca05f9, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-q5jv-m6qw-5g37	A-GOO-TENS-101022/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			611d80db29dd7b0cfb755772c69d60ae5bca05f9. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35996**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `tf.sparse.cross` receives an input `separator` that is not a scalar, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 83dcb4dbfa094e33db084e97c4d0531a559e0ebf. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-p7hr-f446-x6qf, https://github.com/tensorflow/tensorflow/commit/83dcb4dbfa094e33db084e97c4d0531a559e0ebf	A-GOO-TENS-101022/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35997**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `EmptyTensorList` receives an input `element_shape` with more than one dimension, it gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit c8ba76d48567aed347508e0552a257641931024d. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-qhw4-wwr7-gjc5, https://github.com/tensorflow/tensorflow/commit/c8ba76d48567aed347508e0552a257641931024d	A-GOO-TENS-101022/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			range. There are no known workarounds for this issue. **CVE ID : CVE-2022-35998**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Conv2DBackpropInput` receives empty `out_backprop` inputs (e.g. `[3, 1, 0, 1]`), the current CPU/GPU kernels `CHECK` fail (one with dnnl, the other with cudnn). This can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 27a65a43cf763897fecfa5cdb5cc653fc5dd0346. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known	https://github.com/tensorflow/tensorflow/commit/27a65a43cf763897fecfa5cdb5cc653fc5dd0346, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-37jf-mjv6-xfqw	A-GOO-TENS-101022/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-35999**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit aed36912609fc07229b4d0a7b44f3f48efc00fd0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36000**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fqxc-pvf8-2w9v, https://github.com/tensorflow/tensorflow/commit/aed36912609fc07229b4d0a7b44f3f48efc00fd0	A-GOO-TENS-101022/626
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning.	https://github.com/tensorflow/tensorflow/commit/da0d65cdc	A-GOO-TENS-101022/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When `DrawBoundingBoxes` receives an input `boxes` that is not of dtype `float`, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit da0d65cdc1270038e72157ba35bf74b85d9bda11. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36001**	1270038e72157ba35bf74b85d9bda11, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jqm7-m5q7-3hm5	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `Unbatch` receives a nonscalar input `id`, it gives a `CHECK` fail that can trigger a denial of service attack.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mh3m-62v7-68xg, https://github.com/tensorflow/tensorflow/commit/4419d10d576adefa36b0e0	A-GOO-TENS-101022/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We have patched the issue in GitHub commit 4419d10d576adefa36b0e0a9425d2569f7c0189f. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36002**	a9425d2569f7c0189f	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RandomPoissonV2` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-cv2p-32v3-vhwq, https://github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3	A-GOO-TENS-101022/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36003**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.random.gamma` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit 552bfced6ce4809db5f3ca305f60ff80dd40c5a3. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and	https://github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-mv8m-8x97-937q	A-GOO-TENS-101022/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36004**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_min_max_vars_gradient` receives input `min` or `max` that is nonscalar, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit f3cf67ac5705f4f04721d15e485e192bb319feed. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-r26c-679w-mrjm, https://github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319feed	A-GOO-TENS-101022/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36005		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertGenericFunctionToFunctionDef` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit 1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36011**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-fv43-93gv-vm8f, https://github.com/tensorflow/tensorflow/commit/1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b	A-GOO-TENS-101022/632
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::ConvertG	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-jvhc-5hhr-w3v5,	A-GOO-TENS-101022/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enericFunctionToFunctionDef` is given empty function attributes, it crashes. We have patched the issue in GitHub commit ad069af92392efee1418c48ff561fd3070a03d7b. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36012**	https://github.com/tensorflow/tensorflow/commit/ad069af92392efee1418c48ff561fd3070a03d7b	
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::GraphDefImporter::ConvertNodeDef` tries to convert NodeDefs without an op name, it crashes. We have patched the issue in GitHub commit a0f0b9a21c9270930457095092f558fb	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-828c-5j5q-vrjq	A-GOO-TENS-101022/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36013**		
NULL Pointer Dereference	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `mlir::tfg::TFOp::nameAttr` receives null type list attributes, it crashes. We have patched the issue in GitHub commits 3a754740d5414e362512ee981eefba41561a63a6 and a0f0b9a21c9270930457095092f558fbad4c03e5. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/commit/a0f0b9a21c9270930457095092f558fbad4c03e5, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-7j3m-8g3c-9qqq	A-GOO-TENS-101022/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36014**		
Integer Overflow or Wraparound	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `RangeSize` receives values that do not fit into an `int64_t`, it crashes. We have patched the issue in GitHub commit 37e64539cd29fcfb814c4451152a60f5d107b0f0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36015**	https://github.com/tensorflow/tensorflow/security/advisories/GHSA-rh87-q4vg-m45j, https://github.com/tensorflow/tensorflow/commit/37e64539cd29fcfb814c4451152a60f5d107b0f0	A-GOO-TENS-101022/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When `tensorflow::full_type::SubstituteFromAttrs` receives a `FullTypeDef& t` that is not exactly three args, it triggers a `CHECK`-fail instead of returning a status. We have patched the issue in GitHub commit 6104f0d4091c260ce9352f9155f7e9b725eab012. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36016**	https://github.com/tensorflow/tensorflow/commit/6104f0d4091c260ce9352f9155f7e9b725eab012, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-g468-qj8g-vcjc	A-GOO-TENS-101022/637
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `Requantize` is given `input_min`,	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de	A-GOO-TENS-101022/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`input_max`, `requested_output_min`, `requested_output_max` tensors of a nonzero rank, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36017**	849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wqmc-pm8c-2jhc	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `RaggedTensorToVariant` is given a `rt_nested_splits` list that contains tensors of ranks	https://github.com/tensorflow/tensorflow/commit/88f93dfe691563baa4ae1e80ccde2d5c7a143821, https://github.com/tensorflow/tensorflow/sec	A-GOO-TENS-101022/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other than one, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 88f93dfe691563baa4ae1e80ccde2d5c7a143821. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36018**	urity/advisories/GHSA-m6cv-4fmf-66xf	
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `FakeQuantWithMinMaxVarsPerChannel` is given `min` or `max` tensors of a rank other than one, it results in a `CHECK` fail that can be used to trigger a denial of	https://github.com/tensorflow/tensorflow/commit/785d67a78a1d533759fcd2f5e8d6ef778de849e0, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9j4v-pp28-mxv7	A-GOO-TENS-101022/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service attack. We have patched the issue in GitHub commit 785d67a78a1d533759fcd2f5e8d6ef778de849e0. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36019**		
Reachable Assertion	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. If `QuantizeAndDequantizeV3` is given a nonscalar `num_bits` input tensor, it results in a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit f3f9cb38ecfe5a8a703f2c4a8fead434ef	https://github.com/tensorflow/tensorflow/commit/f3f9cb38ecfe5a8a703f2c4a8fead434ef291713, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-9cr2-8pwr-fhfq	A-GOO-TENS-101022/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			291713. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36026**		
N/A	16-Sep-2022	7.5	TensorFlow is an open source platform for machine learning. When converting transposed convolutions using per-channel weight quantization the converter segfaults and crashes the Python process. We have patched the issue in GitHub commit aa0b852a4588cea4d36b74feb05d93055540b450. The fix will be included in TensorFlow 2.10.0. We will also cherrypick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1,	https://github.com/tensorflow/tensorflow/commit/aa0b852a4588cea4d36b74feb05d93055540b450, https://github.com/tensorflow/tensorflow/security/advisories/GHSA-79h2-q768-fpxr	A-GOO-TENS-101022/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue. **CVE ID : CVE-2022-36027**		
Vendor: grafana					
Product: grafana					
Affected Version(s): * Up to (excluding) 8.5.13					
Authentication Bypass by Spoofing	20-Sep-2022	6.6	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.1.6 and 8.5.13 are vulnerable to an escalation from admin to server admin when auth proxy is used, allowing an admin to take over the server admin account and gain full control of the grafana instance. All installations should be upgraded as soon as possible. As a workaround deactivate auth proxy following the instructions at: https://grafana.com/docs/grafana/latest/setup-grafana/configure-	https://github.com/grafana/grafana/security/advisories/GHSA-ff5c-938w-8c9q	A-GRA-GRAF-101022/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security/configure-authentication/auth-proxy/ **CVE ID : CVE-2022-35957**		
Improper Preservation of Permissions	22-Sep-2022	3.8	Grafana is an open-source platform for monitoring and observability. In versions prior to 8.5.13, 9.0.9, and 9.1.6, Grafana is subject to Improper Preservation of Permissions resulting in privilege escalation on some folders where Admin is the only used permission. The vulnerability impacts Grafana instances where RBAC was disabled and enabled afterwards, as the migrations which are translating legacy folder permissions to RBAC permissions do not account for the scenario where the only user permission in the folder is Admin, as a result RBAC adds permissions for Editors and Viewers which allow them to edit	https://github.com/grafana/grafana/security/advisories/GHSA-p978-56hq-r492	A-GRA-GRAF-101022/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and view folders accordingly. This issue has been patched in versions 8.5.13, 9.0.9, and 9.1.6. A workaround when the impacted folder/dashboard is known is to remove the additional permissions manually. **CVE ID : CVE-2022-36062**		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.0.9					
Authentication Bypass by Spoofing	20-Sep-2022	6.6	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.1.6 and 8.5.13 are vulnerable to an escalation from admin to server admin when auth proxy is used, allowing an admin to take over the server admin account and gain full control of the grafana instance. All installations should be upgraded as soon as possible. As a workaround deactivate auth proxy following the instructions at: https://grafana.co	https://github.com/grafana/grafana/security/advisories/GHSA-ff5c-938w-8c9q	A-GRA-GRAF-101022/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m/docs/grafana/latest/setup-grafana/configure-security/configure-authentication/auth-proxy/ **CVE ID : CVE-2022-35957**		
Improper Preservation of Permissions	22-Sep-2022	3.8	Grafana is an open-source platform for monitoring and observability. In versions prior to 8.5.13, 9.0.9, and 9.1.6, Grafana is subject to Improper Preservation of Permissions resulting in privilege escalation on some folders where Admin is the only used permission. The vulnerability impacts Grafana instances where RBAC was disabled and enabled afterwards, as the migrations which are translating legacy folder permissions to RBAC permissions do not account for the scenario where the only user permission in the folder is Admin, as a result RBAC adds permissions for	https://github.com/grafana/grafana/security/advisories/GHSA-p978-56hq-r492	A-GRA-GRAF-101022/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Editors and Viewers which allow them to edit and view folders accordingly. This issue has been patched in versions 8.5.13, 9.0.9, and 9.1.6. A workaround when the impacted folder/dashboard is known is to remove the additional permissions manually. **CVE ID : CVE-2022-36062**		
Affected Version(s): From (including) 9.1.0 Up to (excluding) 9.1.6					
Authentication Bypass by Spoofing	20-Sep-2022	6.6	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.1.6 and 8.5.13 are vulnerable to an escalation from admin to server admin when auth proxy is used, allowing an admin to take over the server admin account and gain full control of the grafana instance. All installations should be upgraded as soon as possible. As a workaround deactivate auth	https://github.com/grafana/grafana/security/advisories/GHSA-ff5c-938w-8c9q	A-GRA-GRAF-101022/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			proxy following the instructions at: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/configure-authentication/auth-proxy/ **CVE ID : CVE-2022-35957**		
Improper Preservation of Permissions	22-Sep-2022	3.8	Grafana is an open-source platform for monitoring and observability. In versions prior to 8.5.13, 9.0.9, and 9.1.6, Grafana is subject to Improper Preservation of Permissions resulting in privilege escalation on some folders where Admin is the only used permission. The vulnerability impacts Grafana instances where RBAC was disabled and enabled afterwards, as the migrations which are translating legacy folder permissions to RBAC permissions do not account for the scenario where the only user permission in the	https://github.com/grafana/grafana/security/advisories/GHSA-p978-56hq-r492	A-GRA-GRAF-101022/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			folder is Admin, as a result RBAC adds permissions for Editors and Viewers which allow them to edit and view folders accordingly. This issue has been patched in versions 8.5.13, 9.0.9, and 9.1.6. A workaround when the impacted folder/dashboard is known is to remove the additional permissions manually. **CVE ID : CVE-2022-36062**		
Vendor: Graphicsmagick					
Product: graphicsmagick					
Affected Version(s): 1.4.020220326					
Out-of-bounds Write	28-Sep-2022	7.8	In GraphicsMagick, a heap buffer overflow was found when parsing MIFF. **CVE ID : CVE-2022-1270**	N/A	A-GRA-GRAP-101022/649
Vendor: gsplugins					
Product: gs_testimonial_slider					
Affected Version(s): * Up to (including) 1.9.6					
Improper Neutralization of Input During Web Page	23-Sep-2022	5.4	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in	https://patchstack.com/database/vulnerability/gs-testimonial/wordpress-gs-	A-GSP-GS_T-101022/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			GS Testimonial Slider plugin <= 1.9.6 at WordPress. **CVE ID : CVE-2022-40213**	testimonial-slider-plugin-1-9-6-multiple-authenticated-stored-cross-site-scripting-xss-vulnerabilities/_s_id=cve, https://wordpress.org/plugins/gs-testimonial/#developers	
Vendor: gunkastudios					
Product: login_block_ips					
Affected Version(s): * Up to (including) 1.0.0					
Cross-Site Request Forgery (CSRF)	26-Sep-2022	4.3	The Login Block IPs WordPress plugin through 1.0.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-3098**	N/A	A-GUN-LOGI-101022/651
Vendor: hanssak					
Product: securegate					
Affected Version(s): 3.5					
Improper Limitation of a Pathname to a Restricted Directory	19-Sep-2022	9.8	This vulnerability of SecureGate is SQL-Injection using login without password. A path traversal vulnerability is also	N/A	A-HAN-SECU-101022/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			identified during file transfer. An attacker can take advantage of these vulnerabilities to perform various attacks such as obtaining privileges and executing remote code, thereby taking over the victim's system. **CVE ID : CVE-2022-23767**		
Product: weblink					
Affected Version(s): From (including) 3.5.2 Up to (including) 3.5.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Sep-2022	9.8	This vulnerability of SecureGate is SQL-Injection using login without password. A path traversal vulnerability is also identified during file transfer. An attacker can take advantage of these vulnerabilities to perform various attacks such as obtaining privileges and executing remote code, thereby taking over the victim's system. **CVE ID : CVE-2022-23767**	N/A	A-HAN-WEBL-101022/653
Vendor: hashicorp					
Product: consul					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.11.9					
Unchecked Return Value	23-Sep-2022	6.5	HashiCorp Consul and Consul Enterprise up to 1.11.8, 1.12.4, and 1.13.1 do not check for multiple SAN URI values in a CSR on the internal RPC endpoint, enabling leverage of privileged access to bypass service mesh intentions. Fixed in 1.11.9, 1.12.5, and 1.13.2." **CVE ID : CVE-2022-40716**	https://discuss.hashicorp.com/t/hcsec-2022-20-consul-service-mesh-intention-bypass-with-malicious-certificate-signing-request/44628, https://discuss.hashicorp.com	A-HAS-CONS-101022/654
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.5					
Unchecked Return Value	23-Sep-2022	6.5	HashiCorp Consul and Consul Enterprise up to 1.11.8, 1.12.4, and 1.13.1 do not check for multiple SAN URI values in a CSR on the internal RPC endpoint, enabling leverage of privileged access to bypass service mesh intentions. Fixed in 1.11.9, 1.12.5, and 1.13.2." **CVE ID : CVE-2022-40716**	https://discuss.hashicorp.com/t/hcsec-2022-20-consul-service-mesh-intention-bypass-with-malicious-certificate-signing-request/44628, https://discuss.hashicorp.com	A-HAS-CONS-101022/655
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.2					
Unchecked Return Value	23-Sep-2022	6.5	HashiCorp Consul and Consul Enterprise up to 1.11.8, 1.12.4, and 1.13.1 do not check	https://discuss.hashicorp.com/t/hcsec-2022-20-consul-service-mesh-	A-HAS-CONS-101022/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for multiple SAN URI values in a CSR on the internal RPC endpoint, enabling leverage of privileged access to bypass service mesh intentions. Fixed in 1.11.9, 1.12.5, and 1.13.2." **CVE ID : CVE-2022-40716**	intention-bypass-with-malicious-certificate-signing-request/44628, https://discuss.hashicorp.com	
Product: vault					
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.10.6					
N/A	22-Sep-2022	9.1	An issue was discovered in HashiCorp Vault and Vault Enterprise before 1.11.3. A vulnerability in the Identity Engine was found where, in a deployment where an entity has multiple mount accessors with shared alias names, Vault may overwrite metadata to the wrong alias due to an issue with checking the proper alias assigned to an entity. This may allow for unintended access to key/value paths using that metadata in Vault.	https://discuss.hashicorp.com/t/hcsec-2022-18-vault-entity-alias-metadata-may-leak-between-aliases-with-the-same-name-assigned-to-the-same-entity/44550, https://discuss.hashicorp.com	A-HAS-VAUL-101022/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40186		
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.3					
N/A	22-Sep-2022	9.1	An issue was discovered in HashiCorp Vault and Vault Enterprise before 1.11.3. A vulnerability in the Identity Engine was found where, in a deployment where an entity has multiple mount accessors with shared alias names, Vault may overwrite metadata to the wrong alias due to an issue with checking the proper alias assigned to an entity. This may allow for unintended access to key/value paths using that metadata in Vault. **CVE ID : CVE-2022-40186**	https://discuss.hashicorp.com/t/hcsec-2022-18-vault-entity-alias-metadata-may-leak-between-aliases-with-the-same-name-assigned-to-the-same-entity/44550, https://discuss.hashicorp.com	A-HAS-VAUL-101022/658
Affected Version(s): From (including) 1.8.0 Up to (excluding) 1.9.9					
N/A	22-Sep-2022	9.1	An issue was discovered in HashiCorp Vault and Vault Enterprise before 1.11.3. A vulnerability in the Identity Engine	https://discuss.hashicorp.com/t/hcsec-2022-18-vault-entity-alias-metadata-may-leak-between-aliases-with-	A-HAS-VAUL-101022/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was found where, in a deployment where an entity has multiple mount accessors with shared alias names, Vault may overwrite metadata to the wrong alias due to an issue with checking the proper alias assigned to an entity. This may allow for unintended access to key/value paths using that metadata in Vault. **CVE ID : CVE-2022-40186**	the-same-name-assigned-to-the-same-entity/44550, https://discuss.hashicorp.com	
Vendor: Haxx					
Product: curl					
Affected Version(s): * Up to (excluding) 7.85.0					
N/A	23-Sep-2022	3.7	When curl is used to retrieve and parse cookies from a HTTP(S) server, itaccepts cookies using control codes that when later are sent back to a HTTPserver might make the server return 400 responses. Effectively allowing a"sister site" to deny service to all siblings.	https://security.netapp.com/advisory/ntap-20220930-0005/	A-HAX-CURL-101022/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35252		
Vendor: heimavista					
Product: dark_horse_rpage					
Affected Version(s): * Up to (excluding) 5.4.103					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	6.1	Heimavista Rpage has insufficient filtering for platform web URL. An unauthenticated remote attacker can inject JavaScript and perform XSS (Reflected Cross-Site Scripting) attack. **CVE ID : CVE-2022-39053**	N/A	A-HEI-DARK-101022/661
Vendor: helpsystems					
Product: cobalt_strike					
Affected Version(s): * Up to (including) 4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	An XSS (Cross Site Scripting) vulnerability was found in HelpSystems Cobalt Strike through 4.7 that allowed a remote attacker to execute HTML on the Cobalt Strike teamserver. To exploit the vulnerability, one must first inspect a Cobalt Strike payload, and then modify the	https://www.cobaltstrike.com/blog/tag/release/, https://www.cobaltstrike.com/blog/out-of-band-update-cobalt-strike-4-7-1/	A-HEL-COBA-101022/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			username field in the payload (or create a new payload with the extracted information and then modify that username field to be malformed). **CVE ID : CVE-2022-39197**		
Vendor: hipcam					
Product: realserver					
Affected Version(s): 1.0					
Use of Insufficiently Random Values	26-Sep-2022	6.5	ieGeek IG20 hipcam RealServer V1.0 is vulnerable to Incorrect Access Control. The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices. **CVE ID : CVE-2022-38970**	N/A	A-HIP-REAL-101022/663
Vendor: Honeywell					
Product: softmaster					
Affected Version(s): 4.51					
Incorrect Permission Assignmen	16-Sep-2022	7.8	A local unprivileged attacker may	https://www.security.honeywell.com/-	A-HON-SOFT-101022/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t for Critical Resource			escalate to administrator privileges in Honeywell SoftMaster version 4.51, due to insecure permission assignment. **CVE ID : CVE-2022-2332**	/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-09-13-02_V4-pdf.pdf, https://www.cisa.gov/uscert/ics/advisories/icsa-22-256-02	
Uncontrolled Search Path Element	16-Sep-2022	7.8	If an attacker manages to trick a valid user into loading a malicious DLL, the attacker may be able to achieve code execution in Honeywell SoftMaster version 4.51 application's context and permissions. **CVE ID : CVE-2022-2333**	https://www.security.honeywell.com/-/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-09-13-02_V4-pdf.pdf, https://www.cisa.gov/uscert/ics/advisories/icsa-22-256-02	A-HON-SOFT-101022/665
Vendor: IBM					
Product: application_gateway					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	5.4	IBM Application Gateway is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading	https://exchange.xforce.ibmcloud.com/vulnerabilities/221965, https://www.ibm.com/support/pages/node/6824247	A-IBM-APPL-101022/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to credentials disclosure within a trusted session. IBM X-Force ID: 221965. **CVE ID : CVE-2022-22387**		
Product: common_cryptographic_architecture					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.7.12					
Improper Input Validation	23-Sep-2022	5.5	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596. **CVE ID : CVE-2022-22423**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223596, https://www.ibm.com/support/pages/node/6695893	A-IBM-COMM-101022/667
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.3.44					
Improper Input Validation	23-Sep-2022	5.5	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596. **CVE ID : CVE-2022-22423**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223596, https://www.ibm.com/support/pages/node/6695893	A-IBM-COMM-101022/668
Product: infosphere_information_server					
Affected Version(s): 11.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236586. **CVE ID : CVE-2022-40748**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236586, https://www.ibm.com/support/pages/node/6695961	A-IBM-INFO-101022/669
Product: jazz_for_service_management					
Affected Version(s): * Up to (excluding) 1.1.3.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	5.4	IBM Jazz for Service Management is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	https://www.ibm.com/support/pages/node/6824117, https://exchange.xforce.ibmcloud.com/vulnerabilities/231381	A-IBM-JAZZ-101022/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 231381. **CVE ID : CVE-2022-35722**		
Affected Version(s): 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	IBM Jazz for Service Management 1.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 231380. **CVE ID : CVE-2022-35721**	https://www.ibm.com/support/pages/node/6695811, https://exchange.xforce.ibmcloud.com/vulnerabilities/231380	A-IBM-JAZZ-101022/671
Product: maximo_asset_management					
Affected Version(s): 7.6.1.1					
Improper Authentication	21-Sep-2022	8.1	IBM Maximo Asset Management 7.6.1.1, 7.6.1.2, and 7.6.1.3 could allow a user to bypass authentication and obtain sensitive information or perform tasks they should not have access to. IBM X-Force ID: 236311.	https://www.ibm.com/support/pages/node/6621599, https://exchange.xforce.ibmcloud.com/vulnerabilities/236311	A-IBM-MAXI-101022/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40616		
Affected Version(s): 7.6.1.2					
Improper Authentication	21-Sep-2022	8.1	IBM Maximo Asset Management 7.6.1.1, 7.6.1.2, and 7.6.1.3 could allow a user to bypass authentication and obtain sensitive information or perform tasks they should not have access to. IBM X-Force ID: 236311. **CVE ID : CVE-2022-40616**	https://www.ibm.com/support/pages/node/6621599, https://exchange.xforce.ibmcloud.com/vulnerabilities/236311	A-IBM-MAXI-101022/673
Affected Version(s): 7.6.1.3					
Improper Authentication	21-Sep-2022	8.1	IBM Maximo Asset Management 7.6.1.1, 7.6.1.2, and 7.6.1.3 could allow a user to bypass authentication and obtain sensitive information or perform tasks they should not have access to. IBM X-Force ID: 236311. **CVE ID : CVE-2022-40616**	https://www.ibm.com/support/pages/node/6621599, https://exchange.xforce.ibmcloud.com/vulnerabilities/236311	A-IBM-MAXI-101022/674
Product: qradar_user_behavior_analytics					
Affected Version(s): * Up to (excluding) 4.1.9					
Exposure of Resource to Wrong Sphere	28-Sep-2022	6.5	IBM QRadar User Behavior Analytics could allow an authenticated user to obtain sensitive information from that they should	https://exchange.xforce.ibmcloud.com/vulnerabilities/232791, https://www.ibm.com/support	A-IBM-QRAD-101022/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not have access to. IBM X-Force ID: 232791. **CVE ID : CVE-2022-36771**	/pages/node/6824197	
Product: spectrum_protect_plus					
Affected Version(s): * Up to (excluding) 10.1.12					
Exposure of Resource to Wrong Sphere	19-Sep-2022	5.9	Versions of IBM Spectrum Protect Plus prior to 10.1.12 (excluding 10.1.12) include the private key information for a certificate inside the generated .crt file when uploading a TLS certificate to IBM Spectrum Protect Plus. If this generated .crt file is shared, an attacker can obtain the private key information for the uploaded certificate. IBM X-Force ID: 235718. **CVE ID : CVE-2022-40234**	https://www.ibm.com/support/pages/node/6619947, https://exchange.xforce.ibmcloud.com/vulnerabilities/235718	A-IBM-SPEC-101022/676
Affected Version(s): From (including) 10.1.6 Up to (including) 10.1.11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Sep-2022	7.5	IBM Spectrum Protect Plus 10.1.6 through 10.1.11 Microsoft File Systems restore operation can download any file on the target machine by manipulating the	https://exchange.xforce.ibmcloud.com/vulnerabilities/235873, https://www.ibm.com/support/pages/node/6620209	A-IBM-SPEC-101022/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL with a directory traversal attack. This results in the restore operation gaining access to files which the operator should not have access to. IBM X-Force ID: 235873. **CVE ID : CVE-2022-40608**		
Product: sterling_partner_engagement_manager					
Affected Version(s): 6.2.1.0					
Improper Restriction of XML External Entity Reference	23-Sep-2022	7.1	IBM Sterling Partner Engagement Manager 6.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 230017. **CVE ID : CVE-2022-34348**	https://www.ibm.com/support/pages/node/6695927, https://exchange.xforce.ibmcloud.com/vulnerabilities/230017	A-IBM-STER-101022/678
Affected Version(s): From (including) 2.0 Up to (excluding) 6.1.2.6					
Improper Restriction of XML External Entity Reference	23-Sep-2022	7.1	IBM Sterling Partner Engagement Manager 6.1 is vulnerable to an XML External Entity Injection	https://www.ibm.com/support/pages/node/6695927, https://exchange.xforce.ibmclou	A-IBM-STER-101022/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 230017. **CVE ID : CVE-2022-34348**	d.com/vulnerabilities/230017	
Affected Version(s): From (including) 6.2.0.0 Up to (excluding) 6.2.0.4					
Improper Restriction of XML External Entity Reference	23-Sep-2022	7.1	IBM Sterling Partner Engagement Manager 6.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 230017. **CVE ID : CVE-2022-34348**	https://www.ibm.com/support/pages/node/6695927, https://exchange.xforce.ibmcloud.com/vulnerabilities/230017	A-IBM-STER-101022/680
Product: websphere_application_server					
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.0.0.45					
Server-Side Request Forgery (SSRF)	28-Sep-2022	6.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to server-side request forgery (SSRF). By	https://exchange.xforce.ibmcloud.com/vulnerabilities/230809, https://www.ibm.com/support	A-IBM-WEBS-101022/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sending a specially crafted request, an attacker with local network access could exploit this vulnerability to obtain sensitive data. **CVE ID : CVE-2022-35282**	/pages/node/6824179	
Affected Version(s): From (including) 8.0.0.0 Up to (excluding) 8.0.0.15					
Server-Side Request Forgery (SSRF)	28-Sep-2022	6.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker with local network access could exploit this vulnerability to obtain sensitive data. **CVE ID : CVE-2022-35282**	https://exchange.xforce.ibmcloud.com/vulnerabilities/230809, https://www.ibm.com/support/pages/node/6824179	A-IBM-WEBS-101022/682
Affected Version(s): From (including) 8.5.0.0 Up to (excluding) 8.5.5.22					
Server-Side Request Forgery (SSRF)	28-Sep-2022	6.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker with local network access could exploit this vulnerability to obtain sensitive data.	https://exchange.xforce.ibmcloud.com/vulnerabilities/230809, https://www.ibm.com/support/pages/node/6824179	A-IBM-WEBS-101022/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35282		
Affected Version(s): From (including) 9.0.0.0 Up to (excluding) 9.0.5.13					
Server-Side Request Forgery (SSRF)	28-Sep-2022	6.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker with local network access could exploit this vulnerability to obtain sensitive data. **CVE ID : CVE-2022-35282**	https://exchange.xforce.ibmcloud.com/vulnerabilities/230809, https://www.ibm.com/support/pages/node/6824179	A-IBM-WEBS-101022/684
Vendor: icecoder					
Product: icecoder					
Affected Version(s): 8.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Sep-2022	7.5	ICEcoder v8.1 allows attackers to execute a directory traversal. **CVE ID : CVE-2022-34026**	http://icecoder.com	A-ICE-ICEC-101022/685
Vendor: identity_and_directory_management_system_project					
Product: identity_and_directory_management_system					
Affected Version(s): * Up to (excluding) 2.1.25					
Improper Limitation of a Pathname to a Restricted	21-Sep-2022	7.5	The Identity and Directory Management System developed by Ã‡ekino Bilgi Teknolojileri	https://www.usom.gov.tr/bildirim/tr-22-0636	A-IDE-IDEN-101022/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			before version 2.1.25 has an unauthenticated Path traversal vulnerability. This has been fixed in the version 2.1.25 **CVE ID : CVE-2022-2265**		
Vendor: ikus-soft					
Product: minarca					
Affected Version(s): * Up to (excluding) 4.2.2					
Weak Password Requirements	22-Sep-2022	9.8	Weak Password Requirements in GitHub repository ikus060/minarca prior to 4.2.2. **CVE ID : CVE-2022-3268**	https://huntr.dev/bounties/00e464ce-53b9-485d-ac62-6467881654c2, https://github.com/ikus060/minarca/commit/7b5c7e6cbd59268d5cd4f1b5f42e721db116f71a	A-IKU-MINA-101022/687
Missing Encryption of Sensitive Data	21-Sep-2022	5.3	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository ikus060/minarca prior to 4.2.2. **CVE ID : CVE-2022-3251**	https://github.com/ikus060/minarca/commit/7b5c7e6cbd59268d5cd4f1b5f42e721db116f71a, https://huntr.dev/bounties/b9a1b411-060b-4235-9426-e39bd0a1d6d9	A-IKU-MINA-101022/688
Product: rdiffweb					
Affected Version(s): * Up to (excluding) 2.4.5					
Cross-Site Request	17-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository	https://huntr.dev/bounties/15c8fd98-7f50-	A-IKU-RDIF-101022/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			ikus060/rdiffweb prior to 2.4.5. **CVE ID : CVE-2022-3232**	4d46-b013-42710af1f99c, https://github.com/ikus060/rdiffweb/commit/422791ea45713aaaa865bdca74addb9fffd93a71	
Affected Version(s): * Up to (excluding) 2.4.6					
Missing Encryption of Sensitive Data	21-Sep-2022	5.3	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository ikus060/rdiffweb prior to 2.4.6. **CVE ID : CVE-2022-3250**	https://huntr.dev/bounties/39889a3f-8bb7-448a-b0d4-a18c671bbd23, https://github.com/ikus060/rdiffweb/commit/ac334dd27ceadac0661b1e2e059a8423433c3fee	A-IKU-RDIF-101022/690
Cross-Site Request Forgery (CSRF)	21-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.6. **CVE ID : CVE-2022-3233**	https://huntr.dev/bounties/5ec206e0-eca0-4957-9af4-fdd9185d1db3, https://github.com/ikus060/rdiffweb/commit/18a5aabd48fa6d2d2771a25f95610c28a1a097ca	A-IKU-RDIF-101022/691
Cross-Site Request Forgery (CSRF)	22-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.6. **CVE ID : CVE-2022-3267**	https://huntr.dev/bounties/7b6ec9f4-4fe9-4716-8dba-3491ffa3f6f2, https://github.com/ikus060/rdiffweb/commit/20fc0d304412c	A-IKU-RDIF-101022/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				c569b21f31e52cb8b94094d6314	
Affected Version(s): * Up to (excluding) 2.4.7					
Session Fixation	23-Sep-2022	9.8	Session Fixation in GitHub repository ikus060/rdiffweb prior to 2.4.7. **CVE ID : CVE-2022-3269**	https://huntr.dev/bounties/67c25969-5e7a-4424-817e-e1a918f63cc6, https://github.com/ikus060/rdiffweb/commit/39e7dcd4a1f44d2a7bd92b79d78a800910b1b22b	A-IKU-RDIF-101022/693
Cross-Site Request Forgery (CSRF)	22-Sep-2022	3.5	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.7. **CVE ID : CVE-2022-3274**	https://github.com/ikus060/rdiffweb/commit/e974df75bdbcff3996ad70bd1b4424ec1485ea3f, https://huntr.dev/bounties/8834c356-4ddb-4be7-898b-d76f480e9c3f	A-IKU-RDIF-101022/694
Affected Version(s): * Up to (excluding) 2.4.8					
N/A	26-Sep-2022	7.5	Improper Handling of Length Parameter Inconsistency in GitHub repository ikus060/rdiffweb prior to 2.4.8. **CVE ID : CVE-2022-3272**	https://github.com/ikus060/rdiffweb/commit/667657c6fe2b336c90be37f37fb92f65df4feee3, https://huntr.dev/bounties/733678b9-daa1-4d6a-875a-382fa09a6e38	A-IKU-RDIF-101022/695
N/A	26-Sep-2022	7.5	Improper Handling of Length	https://huntr.dev/bounties/d8	A-IKU-RDIF-101022/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parameter Inconsistency in GitHub repository ikus060/rdiffweb prior to 2.4.8. **CVE ID : CVE-2022-3290**	b8519d-96a5-484c-8141-624c54290bf5, https://github.com/ikus060/rdiffweb/commit/667657c6fe2b336c90be37f37fb92f65df4feee3	
Allocation of Resources Without Limits or Throttling	26-Sep-2022	7.5	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.4.8. **CVE ID : CVE-2022-3295**	https://huntr.dev/bounties/202dd03a-3d97-4c64-bc73-1a0f36614233, https://github.com/ikus060/rdiffweb/commit/667657c6fe2b336c90be37f37fb92f65df4feee3	A-IKU-RDIF-101022/697
Allocation of Resources Without Limits or Throttling	26-Sep-2022	7.5	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.4.8. **CVE ID : CVE-2022-3298**	https://huntr.dev/bounties/f9fedf94-41c9-49c4-8552-e407123a44e7, https://github.com/ikus060/rdiffweb/commit/626cca1b75b6c587afd4241a9692e8929b1921a5	A-IKU-RDIF-101022/698
Use of Cache Containing Sensitive Information	28-Sep-2022	4.6	Use of Cache Containing Sensitive Information in GitHub repository ikus060/rdiffweb prior to 2.4.8. **CVE ID : CVE-2022-3292**	https://huntr.dev/bounties/e9309018-e94f-4e15-b7d1-5d38b6021c5d, https://github.com/ikus060/rdiffweb/commit/2406780831618405a1311337	A-IKU-RDIF-101022/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				7a784f3102465f40	
Improper Cleanup on Thrown Exception	26-Sep-2022	2.4	Improper Cleanup on Thrown Exception in GitHub repository ikus060/rdiffweb prior to 2.4.8. **CVE ID : CVE-2022-3301**	https://huntr.dev/bounties/d3bf1e5d-055a-44b8-8d60-54ab966ed63a, https://github.com/ikus060/rdiffweb/commit/5ac38b2a75becbab9f948bd5e37ecbcd9f0b362e	A-IKU-RDIF-101022/700
Affected Version(s): 2.4.6					
Cross-Site Request Forgery (CSRF)	21-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.4.6. **CVE ID : CVE-2022-3233**	https://huntr.dev/bounties/5ec206e0-eca0-4957-9af4-fdd9185d1db3, https://github.com/ikus060/rdiffweb/commit/18a5aabd48fa6d2d2771a25f95610c28a1a097ca	A-IKU-RDIF-101022/701
Vendor: Imagemagick					
Product: imagemagick					
Affected Version(s): * Up to (excluding) 6.9.12-62					
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.c	A-IMA-IMAG-101022/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	om/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6903b9e41fe7cb70030e8750	
Affected Version(s): From (including) 7.1.0-0 Up to (excluding) 7.1.0-47					
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.com/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6903b9e41fe7cb70030e8750	A-IMA-IMAG-101022/703
Vendor: Insyde					
Product: insydeh2o					
Affected Version(s): From (including) 5.0 Up to (excluding) 05.09.37					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntimeDxe driver allows an attacker to write fixed or predictable data to SMRAM. Exploiting this	https://www.insyde.com/security-pledge/SA-2022035, https://www.insyde.com/security-pledge	A-INS-INSY-101022/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue could lead to escalating privileges to SMM. **CVE ID : CVE-2022-35893**		
Out-of-bounds Write	21-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution. **CVE ID : CVE-2022-35895**	https://www.insyde.com/security-pledge/SA-2022033, https://www.insyde.com/security-pledge	A-INS-INSY-101022/705
Missing Release of Memory after Effective Lifetime	22-Sep-2022	6	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an attacker-specified buffer, leading to information disclosure. **CVE ID : CVE-2022-35894**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022030	A-INS-INSY-101022/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.0 Up to (excluding) 05.09.38					
N/A	22-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.) **CVE ID : CVE-2022-35408**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022031	A-INS-INSY-101022/707
Affected Version(s): From (including) 5.0 Up to (including) 5.5					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver FwBlockServiceSmm, creating SMM, leads to arbitrary code execution. An	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022029	A-INS-INSY-101022/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can replace the pointer to the UEFI boot service GetVariable with a pointer to malware, and then generate a software SMI. **CVE ID : CVE-2022-36338**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Sep-2022	6	An issue SMM memory leak vulnerability in SMM driver (SMRAM was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An attacker can dump SMRAM contents via the software SMI provided by the FvbServicesRuntimeDxe driver to read the contents of SMRAM, leading to information disclosure. **CVE ID : CVE-2022-35896**	https://www.insyde.com/security-pledge/SA-2022034, https://www.insyde.com/security-pledge	A-INS-INSY-101022/709
Affected Version(s): From (including) 5.1 Up to (excluding) 05.17.37					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntim	https://www.insyde.com/security-pledge/SA-2022035, https://www.insyde.com/security-pledge	A-INS-INSY-101022/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			eDxe driver allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM. **CVE ID : CVE-2022-35893**		
Out-of-bounds Write	21-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution. **CVE ID : CVE-2022-35895**	https://www.insyde.com/security-pledge/SA-2022033, https://www.insyde.com/security-pledge	A-INS-INSY-101022/711
Affected Version(s): From (including) 5.1 Up to (excluding) 5.17.37					
Missing Release of Memory after Effective Lifetime	22-Sep-2022	6	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022030	A-INS-INSY-101022/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker-specified buffer, leading to information disclosure. **CVE ID : CVE-2022-35894**		
Affected Version(s): From (including) 5.1 Up to (excluding) 5.17.38					
N/A	22-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.) **CVE ID : CVE-2022-35408**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022031	A-INS-INSY-101022/713
Affected Version(s): From (including) 5.2 Up to (excluding) 05.27.28					
N/A	22-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An	https://www.insyde.com/security-pledge, https://www.insyde.com/secur	A-INS-INSY-101022/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.) **CVE ID : CVE-2022-35408**	ity-pledge/SA-2022031	
Affected Version(s): From (including) 5.2 Up to (excluding) 05.27.29					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntimeDxe driver allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	https://www.insyde.com/security-pledge/SA-2022035, https://www.insyde.com/security-pledge	A-INS-INSY-101022/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35893		
Out-of-bounds Write	21-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution. **CVE ID : CVE-2022-35895**	https://www.insyde.com/security-pledge/SA-2022033, https://www.insyde.com/security-pledge	A-INS-INSY-101022/716
Missing Release of Memory after Effective Lifetime	22-Sep-2022	6	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an attacker-specified buffer, leading to information disclosure. **CVE ID : CVE-2022-35894**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022030	A-INS-INSY-101022/717
Affected Version(s): From (including) 5.3 Up to (excluding) 05.36.28					
N/A	22-Sep-2022	8.2	An issue was discovered in	https://www.insyde.com/secur	A-INS-INSY-101022/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.) **CVE ID : CVE-2022-35408**	ity-pledge, https://www.insyde.com/security-pledge/SA-2022031	
Affected Version(s): From (including) 5.3 Up to (excluding) 05.36.29					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntimeDxe driver allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to	https://www.insyde.com/security-pledge/SA-2022035, https://www.insyde.com/security-pledge	A-INS-INSY-101022/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalating privileges to SMM. **CVE ID : CVE-2022-35893**		
Out-of-bounds Write	21-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution. **CVE ID : CVE-2022-35895**	https://www.insyde.com/security-pledge/SA-2022033, https://www.insyde.com/security-pledge	A-INS-INSY-101022/720
Missing Release of Memory after Effective Lifetime	22-Sep-2022	6	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an attacker-specified buffer, leading to information disclosure. **CVE ID : CVE-2022-35894**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022030	A-INS-INSY-101022/721
Affected Version(s): From (including) 5.4 Up to (excluding) 05.44.28					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running in the operating system.) **CVE ID : CVE-2022-35408**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022031	A-INS-INSY-101022/722
Affected Version(s): From (including) 5.4 Up to (excluding) 05.44.29					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntimeDxe driver allows an attacker to write fixed or predictable data to SMRAM.	https://www.insyde.com/security-pledge/SA-2022035, https://www.insyde.com/security-pledge	A-INS-INSY-101022/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploiting this issue could lead to escalating privileges to SMM. **CVE ID : CVE-2022-35893**		
Out-of-bounds Write	21-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution. **CVE ID : CVE-2022-35895**	https://www.insyde.com/security-pledge/SA-2022033, https://www.insyde.com/security-pledge	A-INS-INSY-101022/724
Missing Release of Memory after Effective Lifetime	22-Sep-2022	6	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an attacker-specified buffer, leading to information disclosure.	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022030	A-INS-INSY-101022/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35894		
Affected Version(s): From (including) 5.4 Up to (excluding) 05.44.30					
N/A	28-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. There is an SMM memory corruption vulnerability in the Software SMI handler in the PnpSmm driver. **CVE ID : CVE-2022-36448**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022032	A-INS-INSY-101022/726
Affected Version(s): From (including) 5.5 Up to (excluding) 05.52.28					
N/A	22-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM callout vulnerability in the SMM driver in UsbLegacyControlSmm leads to possible arbitrary code execution in SMM and escalation of privileges. An attacker could overwrite the function pointers in the EFI_BOOT_SERVICES table before the USB SMI handler triggers. (This is not exploitable from code running	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022031	A-INS-INSY-101022/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the operating system.) **CVE ID : CVE-2022-35408**		
Affected Version(s): From (including) 5.5 Up to (excluding) 05.52.29					
N/A	23-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. An SMM memory corruption vulnerability in the FvbServicesRuntimeDxe driver allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM. **CVE ID : CVE-2022-35893**	https://www.insyde.com/security-pledge/SA-2022035, https://www.insyde.com/security-pledge	A-INS-INSY-101022/728
Out-of-bounds Write	21-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The FwBlockSericceSmm driver does not properly validate input parameters for a software SMI routine, leading to memory corruption of arbitrary addresses including SMRAM, and possible arbitrary code execution.	https://www.insyde.com/security-pledge/SA-2022033, https://www.insyde.com/security-pledge	A-INS-INSY-101022/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35895		
Missing Release of Memory after Effective Lifetime	22-Sep-2022	6	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. The SMI handler for the FwBlockServiceSmm driver uses an untrusted pointer as the location to copy data to an attacker-specified buffer, leading to information disclosure. **CVE ID : CVE-2022-35894**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022030	A-INS-INSY-101022/730
Affected Version(s): From (including) 5.5 Up to (excluding) 05.52.30					
N/A	28-Sep-2022	8.2	An issue was discovered in Insyde InsydeH2O with kernel 5.0 through 5.5. There is an SMM memory corruption vulnerability in the Software SMI handler in the PnpSmm driver. **CVE ID : CVE-2022-36448**	https://www.insyde.com/security-pledge, https://www.insyde.com/security-pledge/SA-2022032	A-INS-INSY-101022/731
Vendor: interview_management_system_project					
Product: interview_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	19-Sep-2022	7.2	Interview Management System v1.0 was discovered to contain a SQL	N/A	A-INT-INTE-101022/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			injection vulnerability via the component /interview/delete.php?action=deletecand&id=. **CVE ID : CVE-2022-38576**		
Vendor: inventree_project					
Product: inventree					
Affected Version(s): * Up to (excluding) 0.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Sep-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository inventree/inventree prior to 0.8.3. **CVE ID : CVE-2022-3355**	https://huntr.dev/bounties/4b7fb92c-f06b-4bbf-82dc-9f013b30b6a6, https://github.com/inventree/inventree/commit/5a08ef908dd5344b4433436a4679d122f7f99e41	A-INV-INVE-101022/733
Vendor: iris					
Product: isams					
Affected Version(s): 22.2.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Sep-2022	5.4	ISAMS 22.2.3.2 is prone to stored Cross-site Scripting (XSS) attack on the title field for groups, allowing an attacker to store a JavaScript payload that will be executed when another user uses the application. **CVE ID : CVE-2022-37028**	N/A	A-IRI-ISAM-101022/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ISC					
Product: bind					
Affected Version(s): 9.10.5					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/735
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/736
Affected Version(s): 9.10.7					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/738
Affected Version(s): 9.11.12					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/739
Improper Verification of Cryptograp	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a	https://kb.isc.org/docs/cve-2022-38177, http://www.op	A-ISC-BIND-101022/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	enwall.com/lists/oss-security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/741
Affected Version(s): 9.11.14-s1					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2795		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/743
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/744
Affected Version(s): 9.11.19-s1					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/746
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/747
Affected Version(s): 9.11.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/748
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/749
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			named crashes for lack of resources. **CVE ID : CVE-2022-38178**		
Affected Version(s): 9.11.27					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/751
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/752
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	security/2022/09/21/3	
Affected Version(s): 9.11.29					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/754
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/756
Affected Version(s): 9.11.3					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/757
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/759
Affected Version(s): 9.11.35					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/760
Improper Verification of Cryptograp	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/762
Affected Version(s): 9.11.37					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/764
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/765
Affected Version(s): 9.11.5					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/767
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/768
Affected Version(s): 9.11.6					
Uncontrolled Resource	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw	https://kb.isc.org/docs/cve-2022-2795, http://www.op	A-ISC-BIND-101022/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	enwall.com/lists/oss-security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/770
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.11.7					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/772
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/773
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**		
Affected Version(s): 9.11.8					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/775
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/776
Improper Verification of Cryptograp	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	security/2022/09/21/3	
Affected Version(s): 9.16.11					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/778
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/780
Affected Version(s): 9.16.13					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/781
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/783
Affected Version(s): 9.16.14					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/784
Affected Version(s): 9.16.21					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	security/2022/09/21/3	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/786
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/787
Improper Verification of Cryptograp	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/list	A-ISC-BIND-101022/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	s/oss-security/2022/09/21/3	
Affected Version(s): 9.16.32					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/789
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/790
Improper Verification of	21-Sep-2022	7.5	By spoofing the target resolver with responses	https://kb.isc.org/docs/cve-2022-38177,	A-ISC-BIND-101022/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	http://www.openwall.com/lists/oss-security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/792
Affected Version(s): 9.16.8					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2795		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/794
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/795
Affected Version(s): 9.9.12					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	security/2022/09/21/3	
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/797
Affected Version(s): 9.9.13					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/798
Improper Verification of Cryptograp	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a	https://kb.isc.org/docs/cve-2022-38177, http://www.op	A-ISC-BIND-101022/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Signature			malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	enwall.com/lists/oss-security/2022/09/21/3	
Affected Version(s): 9.9.3					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/800
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38177		
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.16.33					
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/802
Affected Version(s): From (including) 9.10.7 Up to (including) 9.10.8					
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/803
Affected Version(s): From (including) 9.11.3 Up to (including) 9.16.32					
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	security/2022/09/21/3	
Affected Version(s): From (including) 9.16.14 Up to (excluding) 9.16.33					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/805
Affected Version(s): From (including) 9.18.0 Up to (excluding) 9.18.7					
Out-of-bounds Read	21-Sep-2022	8.2	The underlying bug might cause read past end of the buffer and either read memory it should not read, or crash the process. **CVE ID : CVE-2022-2881**	https://kb.isc.org/docs/cve-2022-2881, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/806
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance,	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	security/2022/09/21/3	
Missing Release of Memory after Effective Lifetime	21-Sep-2022	7.5	An attacker can leverage this flaw to gradually erode available memory to the point where named crashes for lack of resources. Upon restart the attacker would have to begin again, but nevertheless there is the potential to deny service. **CVE ID : CVE-2022-2906**	https://kb.isc.org/docs/cve-2022-2906, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/808
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/809
Affected Version(s): From (including) 9.19.0 Up to (excluding) 9.19.5					
Out-of-bounds Read	21-Sep-2022	8.2	The underlying bug might cause read past end of the buffer and either read memory it	https://kb.isc.org/docs/cve-2022-2881, http://www.openwall.com/lists/oss-	A-ISC-BIND-101022/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should not read, or crash the process. **CVE ID : CVE-2022-2881**	security/2022/09/21/3	
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/811
Missing Release of Memory after Effective Lifetime	21-Sep-2022	7.5	An attacker can leverage this flaw to gradually erode available memory to the point where named crashes for lack of resources. Upon restart the attacker would have to begin again, but nevertheless there is the potential to deny service. **CVE ID : CVE-2022-2906**	https://kb.isc.org/docs/cve-2022-2906, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/812
Improper Neutralization of Special Elements in Output Used by a Downstrea	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')					
Affected Version(s): From (including) 9.8.4 Up to (including) 9.16.32					
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/814
Affected Version(s): From (including) 9.9.12 Up to (including) 9.9.13					
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	A-ISC-BIND-101022/815
Vendor: ivanti					
Product: endpoint_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2021.1.1					
N/A	23-Sep-2022	6.7	The "LANDesk(R) Management Agent" service exposes a socket and once connected, it is possible to launch commands only for signed executables. This is a security bug that allows a limited user to get escalated admin privileges on their system. **CVE ID : CVE-2022-30121**	https://forums.ivanti.com/s/article/Security-Advisory-for-Ivanti-Endpoint-Manager-Client-CVE-2022-30121?language=en_US	A-IVA-ENDP-101022/816
Affected Version(s): 2021.1.1					
N/A	23-Sep-2022	6.7	The "LANDesk(R) Management Agent" service exposes a socket and once connected, it is possible to launch commands only for signed executables. This is a security bug that allows a limited user to get escalated admin privileges on their system. **CVE ID : CVE-2022-30121**	https://forums.ivanti.com/s/article/Security-Advisory-for-Ivanti-Endpoint-Manager-Client-CVE-2022-30121?language=en_US	A-IVA-ENDP-101022/817
Vendor: jasper_project					
Product: jasper					
Affected Version(s): 3.0.6					
Reachable Assertion	16-Sep-2022	5.5	JasPer 3.0.6 allows denial of service	N/A	A-JAS-JASP-101022/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a reachable assertion in the function inttobits in libjasper/base/jas_image.c. **CVE ID : CVE-2022-40755**		
Vendor: jeesns					
Product: jeesns					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	5.4	A stored cross-site scripting (XSS) vulnerability in the /weibo/list component of Jeesns v2.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload. **CVE ID : CVE-2022-38550**	N/A	A-JEE-JEES-101022/819
Vendor: Jenkins					
Product: anchore_container_image_scanner					
Affected Version(s): * Up to (including) 1.0.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Jenkins Anchore Container Image Scanner Plugin 1.0.24 and earlier does not escape content provided by the Anchore engine API, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2821	A-JEN-ANCH-101022/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control API responses by Anchore engine. **CVE ID : CVE-2022-41225**		
Product: apprenda					
Affected Version(s): * Up to (including) 2.2.0					
Missing Authorization	21-Sep-2022	4.3	A missing permission check in Jenkins Apprenda Plugin 2.2.0 and earlier allows users with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2022-41251**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2710	A-JEN-APPR-101022/821
Product: bigpanda_notifier					
Affected Version(s): * Up to (including) 1.4.0					
Missing Password Field Masking	21-Sep-2022	5.3	Jenkins BigPanda Notifier Plugin 1.4.0 and earlier does not mask the BigPanda API key on the global configuration form, increasing the potential for attackers to observe and capture it. **CVE ID : CVE-2022-41248**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2243	A-JEN-BIGP-101022/822
Insufficiently	21-Sep-2022	4.3	Jenkins BigPanda Notifier Plugin 1.4.0 and earlier stores the	https://www.jenkins.io/security/advisory/2022-09-	A-JEN-BIGP-101022/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			BigPanda API key unencrypted in its global configuration file on the Jenkins controller where they can be viewed by users with access to the Jenkins controller file system. **CVE ID : CVE-2022-41247**	21/#SECURITY-2243	
Product: build-publisher					
Affected Version(s): * Up to (including) 1.22					
Cross-Site Request Forgery (CSRF)	21-Sep-2022	8	A cross-site request forgery (CSRF) vulnerability in Jenkins Build-Publisher Plugin 1.22 and earlier allows attackers to replace any config.xml file on the Jenkins controller file system with an empty file by providing a crafted file name to an API endpoint. **CVE ID : CVE-2022-41232**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2139	A-JEN-BUIL-101022/824
Improper Limitation of a Pathname to a Restricted Directory	21-Sep-2022	5.7	Jenkins Build-Publisher Plugin 1.22 and earlier allows attackers with Item/Configure permission to create or replace	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2139	A-JEN-BUIL-101022/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			any config.xml file on the Jenkins controller file system by providing a crafted file name to an API endpoint. **CVE ID : CVE-2022-41231**		
Incorrect Authorization	21-Sep-2022	4.3	Jenkins Build-Publisher Plugin 1.22 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to obtain names and URLs of Jenkins servers that the plugin is configured to publish builds to, as well as builds pending for publication to those Jenkins servers. **CVE ID : CVE-2022-41230**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-1994	A-JEN-BUIL-101022/826
Product: compuware_common_configuration					
Affected Version(s): * Up to (including) 1.0.14					
Improper Restriction of XML External Entity Reference	21-Sep-2022	9.8	Jenkins Compuware Common Configuration Plugin 1.0.14 and earlier does not configure its XML parser to prevent	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2832	A-JEN-COMP-101022/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XML external entity (XXE) attacks. **CVE ID : CVE-2022-41226**		
Product: cons3rt					
Affected Version(s): * Up to (including) 1.0.0					
Cross-Site Request Forgery (CSRF)	21-Sep-2022	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins CONS3RT Plugin 1.0.0 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2022-41253**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2751	A-JEN-CONS-101022/828
Missing Authorization	21-Sep-2022	6.5	Missing permission checks in Jenkins CONS3RT Plugin 1.0.0 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2751	A-JEN-CONS-101022/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials stored in Jenkins. **CVE ID : CVE-2022-41254**		
Unprotected Storage of Credentials	21-Sep-2022	6.5	Jenkins CONS3RT Plugin 1.0.0 and earlier stores Cons3rt API token unencrypted in job config.xml files on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system. **CVE ID : CVE-2022-41255**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2759	A-JEN-CONS-101022/830
Missing Authorization	21-Sep-2022	4.3	Missing permission checks in Jenkins CONS3RT Plugin 1.0.0 and earlier allows users with Overall/Read permission to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2022-41252**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2752	A-JEN-CONS-101022/831
Product: dotci					
Affected Version(s): * Up to (including) 2.40.00					
Deserialization of Untrusted Data	21-Sep-2022	9.8	Jenkins DotCi Plugin 2.40.00 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types,	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-1737	A-JEN-DOTC-101022/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a remote code execution vulnerability. **CVE ID : CVE-2022-41237**		
Missing Authorization	21-Sep-2022	9.8	A missing permission check in Jenkins DotCi Plugin 2.40.00 and earlier allows unauthenticated attackers to trigger builds of jobs corresponding to the attacker-specified repository for attacker-specified commits. **CVE ID : CVE-2022-41238**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2867	A-JEN-DOTC-101022/833
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Jenkins DotCi Plugin 2.40.00 and earlier does not escape the GitHub user name parameter provided to commit notifications when displaying them in a build cause, resulting in a stored cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-41239**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2884	A-JEN-DOTC-101022/834
Product: extreme-feedback					
Affected Version(s): * Up to (including) 1.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	21-Sep-2022	5.4	A missing permission check in Jenkins extreme-feedback Plugin 1.7 and earlier allows attackers with Overall/Read permission to discover information about job names attached to lamps, discover MAC and IP addresses of existing lamps, and rename lamps. **CVE ID : CVE-2022-41242**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2001	A-JEN-EXTR-101022/835
Product: jenkins					
Affected Version(s): From (including) 2.367 Up to (including) 2.369					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Jenkins 2.367 through 2.369 (both inclusive) does not escape tooltips of the l:helpIcon UI component used for some help icons on the Jenkins web UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control tooltips for this component. **CVE ID : CVE-2022-41224**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2886	A-JEN-JENK-101022/836
Product: ns-nd_integration_performance_publisher					
Affected Version(s): * Up to (including) 4.8.0.129					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	21-Sep-2022	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.129 and earlier allows attackers to connect to an attacker-specified webserver using attacker-specified credentials. **CVE ID : CVE-2022-41227**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2737	A-JEN-NS-N-101022/837
Missing Authorization	21-Sep-2022	8.8	A missing permission check in Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.129 and earlier allows attackers with Overall/Read permissions to connect to an attacker-specified webserver using attacker-specified credentials. **CVE ID : CVE-2022-41228**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2737	A-JEN-NS-N-101022/838
Affected Version(s): * Up to (including) 4.8.0.134					
Improper Neutralization of Input During	21-Sep-2022	5.4	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.134 and	https://www.jenkins.io/security/advisory/2022-09-	A-JEN-NS-N-101022/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			earlier does not escape configuration options of the Execute NetStorm/NetCloud Test build step, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission. **CVE ID : CVE-2022-41229**	21/#SECURITY-2858	
Product: rqm					
Affected Version(s): * Up to (including) 2.8					
Improper Restriction of XML External Entity Reference	21-Sep-2022	9.1	Jenkins RQM Plugin 2.8 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2022-41241**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2805	A-JEN-RQM-101022/840
Product: rundeck					
Affected Version(s): * Up to (including) 3.6.11					
Missing Authorization	21-Sep-2022	8.8	Jenkins Rundeck Plugin 3.6.11 and earlier does not protect access to the /plugin/rundeck/webhook/ endpoint, allowing users with Overall/Read	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2169	A-JEN-RUND-101022/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission to trigger jobs that are configured to be triggerable via Rundeck. **CVE ID : CVE-2022-41234**		
Missing Authorization	21-Sep-2022	4.3	Jenkins Rundeck Plugin 3.6.11 and earlier does not perform Run/Artifacts permission checks in multiple HTTP endpoints, allowing attackers with Item/Read permission to obtain information about build artifacts of a given job, if the optional Run/Artifacts permission is enabled. **CVE ID : CVE-2022-41233**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2170	A-JEN-RUND-101022/842
Product: scm_httpclient					
Affected Version(s): * Up to (including) 1.5					
Cross-Site Request Forgery (CSRF)	21-Sep-2022	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins SCM HttpClient Plugin 1.5 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2708	A-JEN-SCM_-101022/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2022-41249**		
Missing Authorization	21-Sep-2022	6.5	A missing permission check in Jenkins SCM HttpClient Plugin 1.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2022-41250**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2708	A-JEN-SCM_-101022/844
Product: security_inspector					
Affected Version(s): * Up to (including) 117.v6eecc36919c2					
Cross-Site Request Forgery (CSRF)	21-Sep-2022	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Security Inspector Plugin 117.v6eecc36919c2 and earlier allows attackers to replace the generated report stored in a per-session cache and	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2051	A-JEN-SECU-101022/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			displayed to authorized users at the .../report URL with a report based on attacker-specified report generation options. **CVE ID : CVE-2022-41236**		
Product: smalltest					
Affected Version(s): * Up to (including) 1.0.4					
Improper Validation of Certificate with Host Mismatch	21-Sep-2022	8.1	Jenkins SmallTest Plugin 1.0.4 and earlier does not perform hostname validation when connecting to the configured View26 server that could be abused using a man-in-the-middle attack to intercept these connections. **CVE ID : CVE-2022-41243**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2068	A-JEN-SMAL-101022/846
Product: view26_test-reporting					
Affected Version(s): * Up to (including) 1.0.7					
Improper Validation of Certificate with Host Mismatch	21-Sep-2022	8.1	Jenkins View26 Test-Reporting Plugin 1.0.7 and earlier does not perform hostname validation when connecting to the configured View26 server that could be abused using a man-in-the-middle attack to intercept these connections.	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2069	A-JEN-VIEW-101022/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41244		
Product: walti					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Jenkins Walti Plugin 1.0.1 and earlier does not escape the information provided by the Walti API, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide malicious API responses from Walti. **CVE ID : CVE-2022-41240**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-1870	A-JEN-WALT-101022/848
Product: wildfly_deployer					
Affected Version(s): * Up to (including) 1.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Sep-2022	5.3	Jenkins WildFly Deployer Plugin 1.0.2 and earlier implements functionality that allows agent processes to read arbitrary files on the Jenkins controller file system. **CVE ID : CVE-2022-41235**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2645	A-JEN-WILD-101022/849
Product: worksoft_execution_manager					
Affected Version(s): * Up to (including) 10.0.3.503					
Cross-Site Request	21-Sep-2022	8.8	A cross-site request forgery	https://www.jenkins.io/securit	A-JEN-WORK-101022/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			(CSRF) vulnerability in Jenkins Worksoft Execution Manager Plugin 10.0.3.503 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2022-41245**	y/advisory/2022-09-21/#SECURITY-2237	
Missing Authorization	21-Sep-2022	6.5	A missing permission check in Jenkins Worksoft Execution Manager Plugin 10.0.3.503 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2022-41246**	https://www.jenkins.io/security/advisory/2022-09-21/#SECURITY-2237	A-JEN-WORK-101022/851
Vendor: Jetbrains					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: intellij_idea					
Affected Version(s): * Up to (excluding) 2022.2.2					
Uncontrolled Search Path Element	19-Sep-2022	7.8	The installer of JetBrains IntelliJ IDEA before 2022.2.2 was vulnerable to EXE search order hijacking **CVE ID : CVE-2022-40978**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-101022/852
Product: teamcity					
Affected Version(s): * Up to (excluding) 2022.04.4					
Insertion of Sensitive Information into Log File	23-Sep-2022	5.3	In JetBrains TeamCity before 2022.04.4 environmental variables of "password" type could be logged when using custom Perforce executable **CVE ID : CVE-2022-40979**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-101022/853
Vendor: jettison_project					
Product: jettison					
Affected Version(s): * Up to (including) 1.4.0					
Out-of-bounds Write	16-Sep-2022	7.5	Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=46538, https://github.com/jettison-json/jettison/issues/45	A-JET-JETT-101022/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40149**		
Uncontrolled Resource Consumption	16-Sep-2022	7.5	Those using Jettison to parse untrusted XML or JSON data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by Out of memory. This effect may support a denial of service attack. **CVE ID : CVE-2022-40150**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=46549, https://github.com/jettison-json/jettison/issues/45	A-JET-JETT-101022/855
Vendor: jflyfox					
Product: jfinal_cms					
Affected Version(s): 5.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	9.8	JFinal CMS 5.1.0 is vulnerable to SQL Injection. These interfaces do not use the same component, nor do they have filters, but each uses its own SQL concatenation	N/A	A-JFL-JFIN-101022/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			method, resulting in SQL injection. **CVE ID : CVE-2022-37203**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	9.8	Final CMS 5.1.0 is vulnerable to SQL Injection. **CVE ID : CVE-2022-37204**	N/A	A-JFL-JFIN-101022/857
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	8.8	JFinal CMS 5.1.0 is affected by: SQL Injection. These interfaces do not use the same component, nor do they have filters, but each uses its own SQL concatenation method, resulting in SQL injection. **CVE ID : CVE-2022-37205**	N/A	A-JFL-JFIN-101022/858
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-2022	8.8	JFinal CMS 5.1.0 is affected by: SQL Injection. These interfaces do not use the same component, nor do they have filters, but each uses its own SQL concatenation method, resulting in SQL injection. **CVE ID : CVE-2022-37209**	N/A	A-JFL-JFIN-101022/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: joblib_project					
Product: joblib					
Affected Version(s): * Up to (excluding) 1.2.0					
N/A	26-Sep-2022	9.8	The package joblib from 0 and before 1.2.0 are vulnerable to Arbitrary Code Execution via the pre_dispatch flag in Parallel() class due to the eval() statement. **CVE ID : CVE-2022-21797**	https://github.com/joblib/joblib/commit/b90f10efeb670a2cc877fb88ebb3f2019189e059, https://github.com/joblib/joblib/issues/1128, https://github.com/joblib/joblib/pull/1321, https://security.snyk.io/vuln/SNYK-PYTHON-JOBLIB-3027033	A-JOB-JOBL-101022/860
Vendor: kayrasoft					
Product: kayrasoft					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Sep-2022	9.8	Kayrasoft product before version 2 has an unauthenticated SQL Injection vulnerability. This is fixed in version 2. **CVE ID : CVE-2022-2177**	https://www.usom.gov.tr/bildirim/tr-22-0630	A-KAY-KAYR-101022/861
Affected Version(s): 1					
Improper Neutralization of Special Elements used in an	20-Sep-2022	9.8	Kayrasoft product before version 2 has an unauthenticated SQL Injection vulnerability. This	https://www.usom.gov.tr/bildirim/tr-22-0630	A-KAY-KAYR-101022/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			is fixed in version 2. **CVE ID : CVE-2022-2177**		
Vendor: ketchup_restaurant_reservations_project					
Product: ketchup_restaurant_reservations					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	9.8	The Ketchup Restaurant Reservations WordPress plugin through 1.0.0 does not validate and escape some reservation parameters before using them in SQL statements, which could allow unauthenticated attackers to perform SQL Injection attacks **CVE ID : CVE-2022-2754**	N/A	A-KET-KETC-101022/863
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	6.1	The Ketchup Restaurant Reservations WordPress plugin through 1.0.0 does not sanitise and escape some of the reservation user inputs, allowing unauthenticated attackers to perform Cross-Site Scripting attacks logged in admin viewing the	N/A	A-KET-KETC-101022/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious reservation made **CVE ID : CVE-2022-2753**		
Vendor: keylime					
Product: keylime					
Affected Version(s): * Up to (excluding) 6.3.0					
N/A	21-Sep-2022	7.5	A flaw was found in Keylime before 6.3.0. The logic in the Keylime agent for checking for a secure mount can be fooled by previously created unprivileged mounts allowing secrets to be leaked to other processes on the host. **CVE ID : CVE-2022-23948**	https://github.com/keylime/keylime/commit/1a4f31a6368d651222683c9debe7d6832db6f607, https://seclists.org/oss-sec/2022/q1/101, https://github.com/keylime/keylime/commit/d37c406e69cb6689baa2fb7964bad75209703724	A-KEY-KEYL-101022/865
Authentication Bypass by Spoofing	21-Sep-2022	7.5	In Keylime before 6.3.0, unsanitized UUIDs can be passed by a rogue agent and can lead to log spoofing on the verifier and registrar. **CVE ID : CVE-2022-23949**	https://github.com/keylime/keylime/commit/e429e95329fc60608713ddfb82f4a92ee3b3d2d9, https://seclists.org/oss-sec/2022/q1/101, https://github.com/keylime/keylime/commit/65c2b737129b5837f4a03660a	A-KEY-KEYL-101022/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				eb1191ced275a57	
Exposure of Resource to Wrong Sphere	21-Sep-2022	7.5	In Keylime before 6.3.0, Revocation Notifier uses a fixed /tmp path for UNIX domain socket which can allow unprivileged users a method to prohibit keylime operations. **CVE ID : CVE-2022-23950**	https://seclists.org/oss-sec/2022/q1/101, https://github.com/keylime/keylime/commit/ea5d0373fa2c050d5d95404eb779be7e8327b911	A-KEY-KEYL-101022/867
N/A	21-Sep-2022	7.5	In Keylime before 6.3.0, current keylime installer installs the keylime.conf file, which can contain sensitive data, as world-readable. **CVE ID : CVE-2022-23952**	https://seclists.org/oss-sec/2022/q1/101, https://github.com/keylime/keylime/commit/883085d6a4bcea3012729014d5b8e15ecd65fc7c	A-KEY-KEYL-101022/868
N/A	21-Sep-2022	5.5	In Keylime before 6.3.0, quote responses from the agent can contain possibly untrusted ZIP data which can lead to zip bombs. **CVE ID : CVE-2022-23951**	https://seclists.org/oss-sec/2022/q1/101, https://github.com/keylime/keylime/commit/6e44758b64b0ee13564fc46e807f4ba98091c355	A-KEY-KEYL-101022/869
Vendor: kfm_project					
Product: kfm					
Affected Version(s): * Up to (including) 1.4.7					
Improper Neutralizat	23-Sep-2022	6.1	Cross site scripting (XSS) vulnerability	N/A	A-KFM-KFM-101022/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			in kfm through 1.4.7 via crafted GET request to /kfm/index.php. **CVE ID : CVE-2022-40359**		
Vendor: kovidgoyal					
Product: kitty					
Affected Version(s): * Up to (excluding) 0.26.2					
Improper Encoding or Escaping of Output	23-Sep-2022	7.8	In Kitty before 0.26.2, insufficient validation in the desktop notification escape sequence can lead to arbitrary code execution. The user must display attacker-controlled content in the terminal, then click on a notification popup. **CVE ID : CVE-2022-41322**	https://github.com/kovidgoyal/kitty/compare/v0.26.1...v0.26.2, https://github.com/kovidgoyal/kitty/commit/f05783e64d5fa62e1aed603e8d69aced5e49824f, https://sw.kovidgoyal.net/kitty/changelog/#detailed-list-of-changes, https://bugs.gentoo.org/868543	A-KOV-KITT-101022/871
Vendor: kraken					
Product: kraken.io_image_optimizer					
Affected Version(s): * Up to (including) 2.6.5					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kraken.io Image Optimizer plugin <= 2.6.5 at WordPress. **CVE ID : CVE-2022-38454**	https://patchstack.com/database/vulnerability/kraken-image-optimizer/wordpress-kraken-io-image-optimizer-plugin-2-6-5-	A-KRA-KRAK-101022/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cross-site-request-forgery-csrf-vulnerability/_s_id=cve, https://wordpress.org/plugins/kraken-image-optimizer/	
Vendor: Kubernetes					
Product: cri-o					
Affected Version(s): 1.25.0					
Incorrect Permission Assignment for Critical Resource	19-Sep-2022	7.1	Incorrect handling of the supplementary groups in the CRI-O container engine might lead to sensitive information disclosure or possible data modification if an attacker has direct access to the affected container where supplementary groups are used to set access permissions and is able to execute a binary code in that container. **CVE ID : CVE-2022-2995**	https://github.com/cri-o/cri-o/pull/6159	A-KUB-CRI--101022/873
Vendor: labstack					
Product: echo					
Affected Version(s): 4.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	28-Sep-2022	9.6	Labstack Echo v4.8.0 was discovered to contain an open redirect vulnerability via the Static Handler component. This vulnerability can be leveraged by attackers to cause a Server-Side Request Forgery (SSRF). **CVE ID : CVE-2022-40083**	https://github.com/labstack/echo/issues/2259	A-LAB-ECHO-101022/874
Vendor: lcnet					
Product: smart_evision					
Affected Version(s): * Up to (including) 2022.02.21					
Incorrect Authorization	28-Sep-2022	6.5	Smart eVision has inadequate authorization for the database query function. A remote attacker with general user privilege, who is not explicitly authorized to access the information, can access sensitive information. **CVE ID : CVE-2022-39029**	N/A	A-LCN-SMAR-101022/875
Affected Version(s): 2022.02.21					
Improper Limitation of a Pathname to a	28-Sep-2022	9.8	Smart eVision's file acquisition function has a path traversal vulnerability due	N/A	A-LCN-SMAR-101022/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			to insufficient filtering for special characters in the URL parameter. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication, access restricted paths to download and delete arbitrary system files to disrupt service. **CVE ID : CVE-2022-39033**		
Improper Privilege Management	28-Sep-2022	8.8	Smart eVision has an improper privilege management vulnerability. A remote attacker with general user privilege can exploit this vulnerability to escalate to administrator privilege, and then perform arbitrary system command or disrupt service. **CVE ID : CVE-2022-39032**	N/A	A-LCN-SMAR-101022/877
Incorrect Authorization	28-Sep-2022	7.5	smart eVision has inadequate authorization for system information query function. An unauthenticated remote attacker,	N/A	A-LCN-SMAR-101022/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who is not explicitly authorized to access the information, can access sensitive information. **CVE ID : CVE-2022-39030**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	5.4	Smart eVision has insufficient filtering for special characters in the POST Data parameter in the specific function. An unauthenticated remote attacker can inject JavaScript to perform XSS (Stored Cross-Site Scripting) attack. **CVE ID : CVE-2022-39035**	N/A	A-LCN-SMAR-101022/879
Incorrect Authorization	28-Sep-2022	5.3	Smart eVision has insufficient authorization for task acquisition function. An unauthorized remote attacker can exploit this vulnerability to acquire the Session IDs of other general users only. **CVE ID : CVE-2022-39031**	N/A	A-LCN-SMAR-101022/880
Affected Version(s): 2022.03.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	6.5	Smart eVision has a path traversal vulnerability in the Report API function due to insufficient filtering for special characters in URLs. A remote attacker with general user privilege can exploit this vulnerability to bypass authentication, access restricted paths and download system files. **CVE ID : CVE-2022-39034**	N/A	A-LCN-SMAR-101022/881
Vendor: ldap_wp_login_\/_active_directory_integration_project					
Product: ldap_wp_login_\/_active_directory_integration					
Affected Version(s): * Up to (excluding) 3.0.2					
Cross-Site Request Forgery (CSRF)	26-Sep-2022	7.5	The Ldap WP Login / Active Directory Integration WordPress plugin before 3.0.2 does not have any authorisation and CSRF checks when updating it's settings (which are hooked to the init action), allowing unauthenticated attackers to update them. Attackers could set their own LDAP server to be used to	N/A	A-LDA-LDAP-101022/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated users, therefore bypassing the current authentication **CVE ID : CVE-2022-2987**		
Vendor: librenms					
Product: librenms					
Affected Version(s): * Up to (excluding) 22.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Sep-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository librenms/librenms prior to 22.9.0. **CVE ID : CVE-2022-3231**	https://github.com/librenms/librenms/commit/08050020861230ff96a6507b309cc172a9e70af8, https://huntr.dev/bounties/bcb6ee68-1452-4fdb-932a-f1031d10984f	A-LIB-LIBR-101022/883
Vendor: Liferay					
Product: dxp					
Affected Version(s): 7.0					
URL Redirection to Untrusted Site ('Open Redirect')	22-Sep-2022	6.1	HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through 101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes, which allows remote attackers to	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28977-htmlutil.escaperedirect-circumvention-with-multiple-forward-slash	A-LIF-DXP-101022/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect. **CVE ID : CVE-2022-28977**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	5.4	Stored cross-site scripting (XSS) vulnerability in the Site module's user membership administration page in Liferay Portal 7.0.1 through 7.4.1, and Liferay DXP 7.0 before fix pack 102, 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the a user's name. **CVE ID : CVE-2022-28978**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28978-stored-xss-with-user-name-in-site-membership	A-LIF-DXP-101022/885
Affected Version(s): 7.1					
URL Redirection to Untrusted Site ('Open Redirect')	22-Sep-2022	6.1	HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publishe	A-LIF-DXP-101022/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect. **CVE ID : CVE-2022-28977**	r/HbL5mxmVrnXW/content/cve-2022-28977-htmlutil.escaperedirect-circumvention-with-multiple-forward-slash	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Liferay Portal v7.1.0 through v7.4.2 and Liferay DXP 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 was discovered to contain a cross-site scripting (XSS) vulnerability in the Portal Search module's Custom Facet widget. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28979-xss-in-custom-facet-widget, https://issues.liferay.com/browse/LPE-17381	A-LIF-DXP-101022/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into the Custom Parameter Name text field. **CVE ID : CVE-2022-28979**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	5.4	Stored cross-site scripting (XSS) vulnerability in the Site module's user membership administration page in Liferay Portal 7.0.1 through 7.4.1, and Liferay DXP 7.0 before fix pack 102, 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the a user's name. **CVE ID : CVE-2022-28978**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28978-stored-xss-with-user-name-in-site-membership	A-LIF-DXP-101022/888
Affected Version(s): 7.2					
URL Redirection to Untrusted Site ('Open Redirect')	22-Sep-2022	6.1	HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through 101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes,	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28977-htmlutil.escaperedirect-circumvention-with-multiple-forward-slash	A-LIF-DXP-101022/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect. **CVE ID : CVE-2022-28977**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Liferay Portal v7.1.0 through v7.4.2 and Liferay DXP 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 was discovered to contain a cross-site scripting (XSS) vulnerability in the Portal Search module's Custom Facet widget. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Parameter Name text field. **CVE ID : CVE-2022-28979**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28979-xss-in-custom-facet-widget, https://issues.liferay.com/browse/LPE-17381	A-LIF-DXP-101022/890
Improper Neutralization of	22-Sep-2022	5.4	Stored cross-site scripting (XSS) vulnerability in the	https://portal.liferay.dev/learn/security/know	A-LIF-DXP-101022/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site module's user membership administration page in Liferay Portal 7.0.1 through 7.4.1, and Liferay DXP 7.0 before fix pack 102, 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the a user's name. **CVE ID : CVE-2022-28978**	n-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28978-stored-xss-with-user-name-in-site-membership	
Affected Version(s): 7.3					
URL Redirection to Untrusted Site ('Open Redirect')	22-Sep-2022	6.1	HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through 101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3)	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28977-htmlutil.escaperedirect-circumvention-with-multiple-forward-slash	A-LIF-DXP-101022/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			others parameters that rely on HtmlUtil.escapeRedirect. **CVE ID : CVE-2022-28977**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Liferay Portal v7.1.0 through v7.4.2 and Liferay DXP 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 was discovered to contain a cross-site scripting (XSS) vulnerability in the Portal Search module's Custom Facet widget. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Parameter Name text field. **CVE ID : CVE-2022-28979**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28979-xss-in-custom-facet-widget, https://issues.liferay.com/browse/LPE-17381	A-LIF-DXP-101022/893
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	A cross-site scripting (XSS) vulnerability in Liferay Portal v7.3.3 through v7.4.2 and Liferay DXP v7.3 before service pack 3 allows attackers to execute arbitrary web scripts or HTML via a crafted	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28982-reflected-xss-with-tag-name-in-	A-LIF-DXP-101022/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload injected into the name of a tag. **CVE ID : CVE-2022-28982**	%253Cliferay-asset-asset-tags-selector%253E	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	5.4	Stored cross-site scripting (XSS) vulnerability in the Site module's user membership administration page in Liferay Portal 7.0.1 through 7.4.1, and Liferay DXP 7.0 before fix pack 102, 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the a user's name. **CVE ID : CVE-2022-28978**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28978-stored-xss-with-user-name-in-site-membership	A-LIF-DXP-101022/895
Missing Authorization	22-Sep-2022	4.3	The Layout module in Liferay Portal v7.3.3 through v7.4.3.34, and Liferay DXP 7.3 before update 10, and 7.4 before update 35 does not check user permission before showing the preview of a "Content Page" type page, allowing attackers to view unpublished	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-39975	A-LIF-DXP-101022/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"Content Page" pages via URL manipulation. **CVE ID : CVE-2022-39975**		
Affected Version(s): 7.4					
Improper Privilege Management	22-Sep-2022	6.5	The Translation module in Liferay Portal v7.4.3.12 through v7.4.3.36, and Liferay DXP 7.4 update 8 through 36 does not check permissions before allowing a user to export a web content for translation, allowing attackers to download a web content page's XLIFF translation file via crafted URL. **CVE ID : CVE-2022-38512**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-38512	A-LIF-DXP-101022/897
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal v7.4.3.4 and Liferay DXP v7.4 GA allows attackers to execute arbitrary web scripts or HTML via parameters with the filter_ prefix. **CVE ID : CVE-2022-28980**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28980-reflected-xss-with-filter_*-parameters-in-applied-fragment-filters	A-LIF-DXP-101022/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	22-Sep-2022	4.3	The Layout module in Liferay Portal v7.3.3 through v7.4.3.34, and Liferay DXP 7.3 before update 10, and 7.4 before update 35 does not check user permission before showing the preview of a "Content Page" type page, allowing attackers to view unpublished "Content Page" pages via URL manipulation. **CVE ID : CVE-2022-39975**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-39975	A-LIF-DXP-101022/899
Product: liferay_portal					
Affected Version(s): * Up to (excluding) 7.4.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal v7.4.3.4 and Liferay DXP v7.4 GA allows attackers to execute arbitrary web scripts or HTML via parameters with the filter_ prefix. **CVE ID : CVE-2022-28980**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28980-reflected-xss-with-filter_*-parameters-in-applied-fragment-filters	A-LIF-LIFE-101022/900
Affected Version(s): From (including) 7.0.1 Up to (excluding) 7.4.2					
Improper Neutralization of Input	22-Sep-2022	5.4	Stored cross-site scripting (XSS) vulnerability in the Site module's user	https://portal.liferay.dev/learn/security/known-	A-LIF-LIFE-101022/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			membership administration page in Liferay Portal 7.0.1 through 7.4.1, and Liferay DXP 7.0 before fix pack 102, 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 allows remote attackers to inject arbitrary web script or HTML via the a user's name. **CVE ID : CVE-2022-28978**	vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28978-stored-xss-with-user-name-in-site-membership	
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.4.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Liferay Portal v7.1.0 through v7.4.2 and Liferay DXP 7.1 before fix pack 26, 7.2 before fix pack 15, and 7.3 before service pack 3 was discovered to contain a cross-site scripting (XSS) vulnerability in the Portal Search module's Custom Facet widget. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Parameter Name text field.	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28979-xss-in-custom-facet-widget, https://issues.liferay.com/browse/LPE-17381	A-LIF-LIFE-101022/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28979		
Affected Version(s): From (including) 7.3.1 Up to (excluding) 7.4.3.4					
URL Redirection to Untrusted Site ('Open Redirect')	22-Sep-2022	6.1	HtmlUtil.escapeRedirect in Liferay Portal 7.3.1 through 7.4.2, and Liferay DXP 7.0 fix pack 91 through 101, 7.1 fix pack 17 through 25, 7.2 fix pack 5 through 14, and 7.3 before service pack 3 can be circumvented by using multiple forward slashes, which allows remote attackers to redirect users to arbitrary external URLs via the (1) 'redirect` parameter (2) `FORWARD_URL` parameter, and (3) others parameters that rely on HtmlUtil.escapeRedirect. **CVE ID : CVE-2022-28977**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28977-htmlutil.escaperedirect-circumvention-with-multiple-forward-slash	A-LIF-LIFE-101022/903
Affected Version(s): From (including) 7.3.3 Up to (excluding) 7.4.3.35					
Missing Authorization	22-Sep-2022	4.3	The Layout module in Liferay Portal v7.3.3 through v7.4.3.34, and Liferay DXP 7.3 before update 10, and 7.4 before update 35 does not check user	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-39975	A-LIF-LIFE-101022/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission before showing the preview of a "Content Page" type page, allowing attackers to view unpublished "Content Page" pages via URL manipulation. **CVE ID : CVE-2022-39975**		
Affected Version(s): From (including) 7.3.3 Up to (excluding) 7.4.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	A cross-site scripting (XSS) vulnerability in Liferay Portal v7.3.3 through v7.4.2 and Liferay DXP v7.3 before service pack 3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name of a tag. **CVE ID : CVE-2022-28982**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28982-reflected-xss-with-tag-name-in-%253Cliferay-asset-asset-tags-selector%253E	A-LIF-LIFE-101022/905
Affected Version(s): From (including) 7.4.0 Up to (including) 7.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Sep-2022	7.5	Path traversal vulnerability in the Hypermedia REST APIs module in Liferay Portal 7.4.0 through 7.4.2 allows remote attackers to access files outside of com.liferay.headless.discovery.web/M	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-28981-path-traversal-vulnerability-in-	A-LIF-LIFE-101022/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ETA-INF/resources via the `parameter` parameter. **CVE ID : CVE-2022-28981**	hypermedia-rest-apis	
Affected Version(s): From (including) 7.4.3.12 Up to (including) 7.4.3.36					
Improper Privilege Management	22-Sep-2022	6.5	The Translation module in Liferay Portal v7.4.3.12 through v7.4.3.36, and Liferay DXP 7.4 update 8 through 36 does not check permissions before allowing a user to export a web content for translation, allowing attackers to download a web content page's XLIFF translation file via crafted URL. **CVE ID : CVE-2022-38512**	https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/cve-2022-38512	A-LIF-LIFE-101022/907
Vendor: linux-pam					
Product: linux-pam					
Affected Version(s): * Up to (excluding) 1.5.2-6.1					
Incorrect Authorization	19-Sep-2022	9.8	The Linux-PAM package before 1.5.2-6.1 for openSUSE Tumbleweed allows authentication bypass for SSH logins. The pam_access.so module doesn't correctly restrict login if a user tries	https://www.suse.com/security/cve/CVE-2022-28321.html, http://download.opensuse.org/source/distribution/openSUSE-current/repo/oss/src/, https://bugzilla.suse.com/show	A-LIN-LINU-101022/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to connect from an IP address that is not resolvable via DNS. In such conditions, a user with denied access to a machine can still get access. NOTE: the relevance of this issue is largely limited to openSUSE Tumbleweed and openSUSE Factory; it does not affect Linux-PAM upstream. **CVE ID : CVE-2022-28321**	_bug.cgi?id=1197654	
Vendor: Linuxfoundation					
Product: besu					
Affected Version(s): 22.4.0					
Incorrect Conversion between Numeric Types	24-Sep-2022	9.1	Besu is a Java-based Ethereum client. In versions newer than 22.1.3 and prior to 22.7.1, Besu is subject to an Incorrect Conversion between Numeric Types. An error in 32 bit signed and unsigned types in the calculation of available gas in the CALL operations (including DELEGATECALL) results in incorrect gas being passed	https://github.com/hyperledger/besu/security/advisories/GHSA-4456-w38r-m53x	A-LIN-BESU-101022/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into called contracts and incorrect gas being returned after call execution. Where the amount of gas makes a difference in the success or failure, or if the gas is a negative 64 bit value, the execution will result in a different state root than expected, resulting in a consensus failure in networks with multiple EVM implementations. In networks with a single EVM implementation this can be used to execute with significantly more gas than then transaction requested, possibly exceeding gas limitations. This issue is patched in version 22.7.1. As a workaround, reverting to version 22.1.3 or earlier will prevent incorrect execution. **CVE ID : CVE-2022-36025**		
Affected Version(s): From (including) 22.4.1 Up to (excluding) 22.7.1					
Incorrect Conversion	24-Sep-2022	9.1	Besu is a Java-based Ethereum	https://github.com/hyperledge	A-LIN-BESU-101022/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
between Numeric Types			client. In versions newer than 22.1.3 and prior to 22.7.1, Besu is subject to an Incorrect Conversion between Numeric Types. An error in 32 bit signed and unsigned types in the calculation of available gas in the CALL operations (including DELEGATECALL) results in incorrect gas being passed into called contracts and incorrect gas being returned after call execution. Where the amount of gas makes a difference in the success or failure, or if the gas is a negative 64 bit value, the execution will result in a different state root than expected, resulting in a consensus failure in networks with multiple EVM implementations. In networks with a single EVM implementation this can be used to execute with significantly more gas than then transaction	r/besu/security/advisories/GHSA-4456-w38r-m53x	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requested, possibly exceeding gas limitations. This issue is patched in version 22.7.1. As a workaround, reverting to version 22.1.3 or earlier will prevent incorrect execution. **CVE ID : CVE-2022-36025**		
Product: fabric					
Affected Version(s): * Up to (excluding) 2.4.0					
N/A	23-Sep-2022	7.5	A vulnerability exists in Hyperledger Fabric <2.4 could allow an attacker to construct a non-validated request that could cause a denial of service attack. **CVE ID : CVE-2022-35253**	https://github.com/hyperledger/fabric/pull/3577, https://github.com/hyperledger/fabric/pull/3576, https://github.com/hyperledger/fabric/pull/3572	A-LIN-FABR-101022/911
Vendor: login_no_captcha_recaptcha_project					
Product: login_no_captcha_recaptcha					
Affected Version(s): * Up to (excluding) 1.7					
Authorization Bypass Through User-Controlled Key	16-Sep-2022	4.3	The Login No Captcha reCAPTCHA WordPress plugin before 1.7 doesn't check the proper IP address allowing attackers to spoof IP addresses on the allow list and bypass the need for	https://wpscan.com/vulnerability/5231ac18-ea9a-4bb9-af9f-e3d95a3b54f1	A-LOG-LOGI-101022/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			captcha on the login screen. **CVE ID : CVE-2022-2913**		
Vendor: loqate					
Product: loqate					
Affected Version(s): * Up to (including) 1.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	4.8	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PCA Predict plugin <= 1.0.3 at WordPress. **CVE ID : CVE-2022-40195**	https://patchstack.com/database/vulnerability/address-email-and-phone-validation/wordpress-pca-predict-plugin-1-0-3-authenticated-stored-cross-site-scripting-xss-vulnerability/_s_id=cve, https://wordpress.org/plugins/address-email-and-phone-validation/	A-LOQ-LOQA-101022/913
Vendor: Mailcow					
Product: mailcow					
Affected Version(s): _dockerized Up to (excluding) 2022-09					
URL Redirection to Untrusted Site ('Open Redirect')	27-Sep-2022	8.2	mailcow is a mailserver suite. A vulnerability innversions prior to 2022-09 allows an attacker to craft a custom Swagger API template to spoof Authorize links. This could redirect a victim to	https://github.com/mailcow/mailcow-dockerized/pull/4766, https://github.com/mailcow/mailcow-dockerized/security/advisories	A-MAI-MAIL-101022/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker controller place to steal Swagger authorization credentials or create a phishing page to steal other information. The issue has been fixed with the 2022-09 mailcow Mootember Update. As a workaround, one may delete the Swapper API Documentation from their e-mail server. **CVE ID : CVE-2022-39258**	/GHSA-vjgf-cp5p-wm45	
Vendor: mailoptin					
Product: mailoptin					
Affected Version(s): * Up to (including) 1.2.49.0					
Missing Authorization	23-Sep-2022	5.3	Unauthenticated Optin Campaign Cache Deletion vulnerability in MailOptin plugin <= 1.2.49.0 at WordPress. **CVE ID : CVE-2022-36340**	https://plugins.svn.wordpress.org/mailoptin/trunk/changelog.txt, https://patchstack.com/database/vulnerability/mailoptin/wordpress-mailoptin-plugin-1-2-49-0-unauthenticated-optin-campaign-cache-deletion-	A-MAI-MAIL-101022/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				vulnerability/_s_id=cve	
Vendor: makedeb					
Product: mist					
Affected Version(s): * Up to (excluding) 0.9.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Sep-2022	7.8	Mist is the command-line interface for the makedeb Package Repository. Prior to version 0.9.5, a user-provided `sudo` binary via the `PATH` variable can allow a local user to run arbitrary commands on the user's system with root permissions. Versions 0.9.5 and later contain a patch. No known workarounds exist. **CVE ID : CVE-2022-39245**	https://github.com/makedeb/mist/security/advisories/GHSA-pxg4-7c7r-2ww6, https://github.com/makedeb/mist/commit/e257561a32cffe3c541b265097959adaea3d6b67	A-MAK-MIST-101022/916
Vendor: Matrix					
Product: javascript_sdk					
Affected Version(s): * Up to (excluding) 19.7.0					
Improper Authentication	28-Sep-2022	7.5	Matrix Javascript SDK is the Matrix Client-Server SDK for JavaScript. Prior to version 19.7.0, an attacker cooperating with a malicious homeserver can construct messages appearing to have come from another	https://github.com/matrix-org/matrix-js-sdk/commit/a587d7c36026fe1fcf93dfff63588abee359be76, https://github.com/matrix-org/matrix-js-sdk/security/advisories/GHSA-	A-MAT-JAVA-101022/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person. Such messages will be marked with a grey shield on some platforms, but this may be missing in others. This attack is possible due to the matrix-js-sdk implementing a too permissive key forwarding strategy on the receiving end. Starting with version 19.7.0, the default policy for accepting key forwards has been made more strict in the matrix-js-sdk. matrix-js-sdk will now only accept forwarded keys in response to previously issued requests and only from own, verified devices. The SDK now sets a `trusted` flag on the decrypted message upon decryption, based on whether the key used to decrypt the message was received from a trusted source. Clients need to ensure that messages decrypted with a key with `trusted =	6263-x97c-c4gg, https://github.com/matrix-org/matrix-spec-proposals/pull/3061	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			false` are decorated appropriately, for example, by showing a warning for such messages. This attack requires coordination between a malicious homeserver and an attacker, and those who trust your homeservers do not need a workaround. **CVE ID : CVE-2022-39249**		
Improper Authentication	28-Sep-2022	7.5	Matrix Javascript SDK is the Matrix Client-Server SDK for JavaScript. Prior to version 19.7.0, an attacker cooperating with a malicious homeserver can construct messages that legitimately appear to have come from another person, without any indication such as a grey shield. Additionally, a sophisticated attacker cooperating with a malicious homeserver could employ this vulnerability to perform a targeted	https://github.com/matrix-org/matrix-js-sdk/commit/a587d7c36026fe1fcf93dfff63588abee359be76, https://matrix.org/blog/2022/09/28/upgrade-now-to-address-encryption-vulns-in-matrix-sdks-and-clients	A-MAT-JAVA-101022/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack in order to send fake to-device messages appearing to originate from another user. This can allow, for example, to inject the key backup secret during a self-verification, to make a targeted device start using a malicious key backup spoofed by the homeserver. These attacks are possible due to a protocol confusion vulnerability that accepts to-device messages encrypted with Megolm instead of Olm. Starting with version 19.7.0, matrix-js-sdk has been modified to only accept Olm-encrypted to-device messages. Out of caution, several other checks have been audited or added. This attack requires coordination between a malicious home server and an attacker, so those who trust their home servers do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not need a workaround. **CVE ID : CVE-2022-39251**		
Affected Version(s): 17.1.0					
N/A	28-Sep-2022	5.3	Matrix Javascript SDK is the Matrix Client-Server SDK for JavaScript. Starting with version 17.1.0-rc.1, improperly formed beacon events can disrupt or impede the matrix-js-sdk from functioning properly, potentially impacting the consumer's ability to process data safely. Note that the matrix-js-sdk can appear to be operating normally but be excluding or corrupting runtime data presented to the consumer. This is patched in matrix-js-sdk v19.7.0. Redacting applicable events, waiting for the sync processor to store data, and restarting the client are possible workarounds. Alternatively, redacting the applicable events and clearing all	https://github.com/matrix-org/matrix-js-sdk/commit/a587d7c36026fe1fcf93dfff63588abee359be76, https://github.com/matrix-org/matrix-spec-proposals/pull/3488, https://github.com/matrix-org/matrix-js-sdk/security/advisories/GHSA-hvv8-5v86-r45x	A-MAT-JAVA-101022/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			storage will fix the further perceived issues. Downgrading to an unaffected version, noting that such a version may be subject to other vulnerabilities, will additionally resolve the issue. **CVE ID : CVE-2022-39236**		
Affected Version(s): From (including) 17.1.0 Up to (excluding) 19.7.0					
N/A	28-Sep-2022	5.3	Matrix Javascript SDK is the Matrix Client-Server SDK for JavaScript. Starting with version 17.1.0-rc.1, improperly formed beacon events can disrupt or impede the matrix-js-sdk from functioning properly, potentially impacting the consumer's ability to process data safely. Note that the matrix-js-sdk can appear to be operating normally but be excluding or corrupting runtime data presented to the consumer. This is patched in matrix-js-sdk v19.7.0. Redacting applicable events, waiting for the	https://github.com/matrix-org/matrix-js-sdk/commit/a587d7c36026fe1fcf93dfff63588abee359be76, https://github.com/matrix-org/matrix-spec-proposals/pull/3488, https://github.com/matrix-org/matrix-js-sdk/security/advisories/GHSA-hvv8-5v86-r45x	A-MAT-JAVA-101022/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync processor to store data, and restarting the client are possible workarounds. Alternatively, redacting the applicable events and clearing all storage will fix the further perceived issues. Downgrading to an unaffected version, noting that such a version may be subject to other vulnerabilities, will additionally resolve the issue. **CVE ID : CVE-2022-39236**		
Product: software_development_kit					
Affected Version(s): * Up to (excluding) 0.23.19					
Improper Authentication	28-Sep-2022	7.5	Matrix iOS SDK allows developers to build iOS apps compatible with Matrix. Prior to version 0.23.19, an attacker cooperating with a malicious homeserver can construct messages that legitimately appear to have come from another person, without any indication such as a grey shield. Additionally, a sophisticated	https://matrix.org/blog/2022/09/28/upgrade-now-to-address-encryption-vulns-in-matrix-sdks-and-clients, https://github.com/matrix-org/matrix-ios-sdk/security/advisories/GHSA-hw6g-j8v6-9hcm	A-MAT-SOFT-101022/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker cooperating with a malicious homeserver could employ this vulnerability to perform a targeted attack in order to send fake to-device messages appearing to originate from another user. This can allow, for example, to inject the key backup secret during a self-verification, to make a targeted device start using a malicious key backup spoofed by the homeserver. These attacks are possible due to a protocol confusion vulnerability that accepts to-device messages encrypted with Megolm instead of Olm. matrix-ios-sdk version 0.23.19 has been modified to only accept Olm-encrypted to-device messages. Out of caution, several other checks have been audited or added. This attack requires coordination		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between a malicious home server and an attacker, so those who trust their home servers do not need a workaround. To avoid malicious backup attacks, one should not verify one's new logins using emoji/QR verifications methods until patched. **CVE ID : CVE-2022-39255**		
Improper Authentication	28-Sep-2022	7.5	Matrix iOS SDK allows developers to build iOS apps compatible with Matrix. Prior to version 0.23.19, an attacker cooperating with a malicious homeserver can construct messages appearing to have come from another person. Such messages will be marked with a grey shield on some platforms, but this may be missing in others. This attack is possible due to the matrix-ios-sdk implementing a too permissive key forwarding	https://matrix.org/blog/2022/09/28/upgrade-now-to-address-encryption-vulns-in-matrix-sdks-and-clients, https://github.com/matrix-org/matrix-ios-sdk/security/advisories/GHSA-qxr3-5jmq-xcf4	A-MAT-SOFT-101022/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			strategy. The default policy for accepting key forwards has been made more strict in the matrix-ios-sdk version 0.23.19. matrix-ios-sdk will now only accept forwarded keys in response to previously issued requests and only from own, verified devices. The SDK now sets a `trusted` flag on the decrypted message upon decryption, based on whether the key used to decrypt the message was received from a trusted source. Clients need to ensure that messages decrypted with a key with `trusted = false` are decorated appropriately (for example, by showing a warning for such messages). This attack requires coordination between a malicious home server and an attacker, so those who trust their home servers do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not need a workaround. **CVE ID : CVE-2022-39257**		
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Authentication	28-Sep-2022	7.5	matrix-android-sdk2 is the Matrix SDK for Android. Prior to version 1.5.1, an attacker cooperating with a malicious homeserver can construct messages that legitimately appear to have come from another person, without any indication such as a grey shield. Additionally, a sophisticated attacker cooperating with a malicious homeserver could employ this vulnerability to perform a targeted attack in order to send fake to-device messages appearing to originate from another user. This can allow, for example, to inject the key backup secret during a self-verification, to make a targeted device start using a malicious key	https://matrix.org/blog/2022/09/28/upgrade-now-to-address-encryption-vulns-in-matrix-sdks-and-clients, https://github.com/matrix-org/matrix-android-sdk2/security/advisories/GHSA-fpgf-pjjv-2qgm	A-MAT-SOFT-101022/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backup spoofed by the homeserver. matrix-android-sdk2 would then additionally sign such a key backup with its device key, spilling trust over to other devices trusting the matrix-android-sdk2 device. These attacks are possible due to a protocol confusion vulnerability that accepts to-device messages encrypted with Megolm instead of Olm. matrix-android-sdk2 version 1.5.1 has been modified to only accept Olm-encrypted to-device messages and to stop signing backups on a successful decryption. Out of caution, several other checks have been audited or added. This attack requires coordination between a malicious home server and an attacker, so those who trust their home servers do		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not need a workaround. **CVE ID : CVE-2022-39248**		
Improper Authentication	28-Sep-2022	5.3	matrix-android-sdk2 is the Matrix SDK for Android. Prior to version 1.5.1, an attacker cooperating with a malicious homeserver can construct messages appearing to have come from another person. Such messages will be marked with a grey shield on some platforms, but this may be missing in others. This attack is possible due to the key forwarding strategy implemented in the matrix-android-sdk2 that is too permissive. Starting with version 1.5.1, the default policy for accepting key forwards has been made more strict in the matrix-android-sdk2. The matrix-android-sdk2 will now only accept forwarded keys in response to previously issued requests and only	https://github.com/matrix-org/matrix-android-sdk2/security/advisories/GHSA-2pvj-p485-cp3m, https://github.com/matrix-org/matrix-android-sdk2/commit/77df720a238d17308deab83ecaa37f7a4740a17e, https://github.com/matrix-org/matrix-spec-proposals/pull/3061	A-MAT-SOFT-101022/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from own, verified devices. The SDK now sets a `trusted` flag on the decrypted message upon decryption, based on whether the key used to decrypt the message was received from a trusted source. Clients need to ensure that messages decrypted with a key with `trusted = false` are decorated appropriately (for example, by showing a warning for such messages). As a workaroubnd, current users of the SDK can disable key forwarding in their forks using `CryptoService#enableKeyGossiping( enable: Boolean)`. **CVE ID : CVE-2022-39246**		
Vendor: mattermost					
Product: mattermost_server					
Affected Version(s): * Up to (excluding) 7.2.0					
Unrestricted Upload of File with Dangerous Type	23-Sep-2022	6.5	Mattermost version 7.1.x and earlier fails to sufficiently process a specifically crafted GIF file when it is uploaded	https://mattermost.com/security-updates/	A-MAT-MATT-101022/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while drafting a post, which allows authenticated users to cause resource exhaustion while processing the file, resulting in server-side Denial of Service. **CVE ID : CVE-2022-3257**		
Vendor: Maxfoundry					
Product: maxbuttons					
Affected Version(s): * Up to (including) 9.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	4.8	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Max Foundry Button Plugin MaxButtons plugin <= 9.2 at WordPress **CVE ID : CVE-2022-38703**	https://patchstack.com/database/vulnerability/maxbuttons/wordpress-wordpress-button-plugin-maxbuttons-plugin-9-2-authenticated-stored-cross-site-scripting-xss-vulnerability/_s_id=cve, https://wordpress.org/plugins/maxbuttons/#developers	A-MAX-MAXB-101022/926
Vendor: mcwebserver_minecraft_mod_for_fabric_and_quilt_project					
Product: mcwebserver_minecraft_mod_for_fabric_and_quilt					
Affected Version(s): * Up to (including) 0.1.2.1					
Improper Limitation of a Pathname	21-Sep-2022	7.5	McWebserver mod runs a simple HTTP server alongside the	https://github.com/J-onasJones/McWebserver/securi	A-MCW-MCWE-101022/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Minecraft server in seperate threads. Path traversal in McWebserver Minecraft Mod for Fabric and Quilt up to and including 0.1.2.1 and McWebserver Minecraft Mod for Forge up to and including 0.1.1 allows all files, accessible by the program, to be read by anyone via HTTP request. Version 0.2.0 with patches are released to both platforms (Fabric and Quilt, Forge). As a workaround, the McWebserver mod can be disabled by removing the file from the `mods` directory. **CVE ID : CVE-2022-39221**	ty/advisories/GHSA-gcvq-42cx-r46q, https://github.com/J-onasJones/McWebserver/pull/1	
Vendor: mcwebserver_minecraft_mod_for_forge_project					
Product: mcwebserver_minecraft_mod_for_forge					
Affected Version(s): * Up to (including) 0.1.1					
Improper Limitation of a Pathname to a Restricted Directory	21-Sep-2022	7.5	McWebserver mod runs a simple HTTP server alongside the Minecraft server in seperate threads. Path traversal in McWebserver	https://github.com/J-onasJones/McWebserver/security/advisories/GHSA-gcvq-42cx-r46q, https://github.c	A-MCW-MCWE-101022/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Minecraft Mod for Fabric and Quilt up to and including 0.1.2.1 and McWebserver Minecraft Mod for Forge up to and including 0.1.1 allows all files, accessible by the program, to be read by anyone via HTTP request. Version 0.2.0 with patches are released to both platforms (Fabric and Quilt, Forge). As a workaround, the McWebserver mod can be disabled by removing the file from the `mods` directory. **CVE ID : CVE-2022-39221**	om/J-onasJones/McWebserver/pull/1	
Vendor: md2roff_project					
Product: md2roff					
Affected Version(s): 1.9					
Out-of-bounds Write	21-Sep-2022	9.8	** DISPUTED ** md2roff 1.9 has a stack-based buffer overflow via a Markdown file, a different vulnerability than CVE-2022-34913. NOTE: the vendor's position is that the product is not	N/A	A-MD2-MD2R-101022/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended for untrusted input. **CVE ID : CVE-2022-41220**		
Vendor: Measuresoft					
Product: scadapro_server					
Affected Version(s): 6.7					
Incorrect Default Permissions	23-Sep-2022	7.8	The security descriptor of Measuresoft ScadaPro Server version 6.7 has inconsistent permissions, which could allow a local user with limited privileges to modify the service binary path and start malicious commands with SYSTEM privileges. **CVE ID : CVE-2022-3263**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-265-01	A-MEA-SCAD-101022/930
Vendor: Mediawiki					
Product: mediawiki					
Affected Version(s): * Up to (excluding) 1.35.6					
Release of Invalid Pointer or Reference	19-Sep-2022	7.5	A denial-of-service issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. When many files exist, requesting Special:NewFiles with actor as a condition can result in a very	https://phabricator.wikimedia.org/T297731	A-MED-MEDI-101022/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			long running query. **CVE ID : CVE-2022-28203**		
Uncontrolled Recursion	19-Sep-2022	4.4	An issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. Users with the editinterface permission can trigger infinite recursion, because a bare local interwiki is mishandled for the mainpage message. **CVE ID : CVE-2022-28201**	https://phabricator.wikimedia.org/T297571	A-MED-MEDI-101022/932
Affected Version(s): From (including) 1.36.0 Up to (excluding) 1.36.4					
Release of Invalid Pointer or Reference	19-Sep-2022	7.5	A denial-of-service issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. When many files exist, requesting Special:NewFiles with actor as a condition can result in a very long running query. **CVE ID : CVE-2022-28203**	https://phabricator.wikimedia.org/T297731	A-MED-MEDI-101022/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Recursion	19-Sep-2022	4.4	An issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. Users with the editinterface permission can trigger infinite recursion, because a bare local interwiki is mishandled for the mainpage message. **CVE ID : CVE-2022-28201**	https://phabricator.wikimedia.org/T297571	A-MED-MEDI-101022/934
Affected Version(s): From (including) 1.37.0 Up to (excluding) 1.37.2					
Release of Invalid Pointer or Reference	19-Sep-2022	7.5	A denial-of-service issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. When many files exist, requesting Special:NewFiles with actor as a condition can result in a very long running query. **CVE ID : CVE-2022-28203**	https://phabricator.wikimedia.org/T297731	A-MED-MEDI-101022/935
N/A	19-Sep-2022	7.5	A denial-of-service issue was discovered in MediaWiki 1.37.x before 1.37.2. Rendering of	https://phabricator.wikimedia.org/T297754	A-MED-MEDI-101022/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			w/index.php?title=Special%3AWhatLinksHere&target=Property%3AP31&namespace=1&invert=1 can take more than thirty seconds. There is a DDoS risk. **CVE ID : CVE-2022-28204**		
Uncontrolled Recursion	19-Sep-2022	4.4	An issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. Users with the editinterface permission can trigger infinite recursion, because a bare local interwiki is mishandled for the mainpage message. **CVE ID : CVE-2022-28201**	https://phabricator.wikimedia.org/T297571	A-MED-MEDI-101022/937
Vendor: Microsoft					
Product: endpoint_configuration_manager					
Affected Version(s): From (including) 2103 Up to (including) 2207					
N/A	20-Sep-2022	7.5	Microsoft Endpoint Configuration Manager Spoofing Vulnerability. **CVE ID : CVE-2022-37972**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37972	A-MIC-ENDP-101022/938
Product: windows_defender_for_endpoint					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Sep-2022	4.7	A time-of-check-time-of-use (TOCTOU) race condition vulnerability was found in networkd-dispatcher. This flaw exists because there is a certain time between the scripts being discovered and them being run. An attacker can abuse this vulnerability to replace scripts that networkd-dispatcher believes to be owned by root with ones that are not. **CVE ID : CVE-2022-29800**	https://www.microsoft.com/security/blog/2022/04/26/microsoft-finds-new-elevation-of-privilege-linux-vulnerability-nimbuspwn/	A-MIC-WIND-101022/939
Affected Version(s): *					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Sep-2022	5.5	A vulnerability was found in networkd-dispatcher. This flaw exists because no functions are sanitized by the OperationalState or the AdministrativeState of networkd-dispatcher. This attack leads to a directory traversal to escape from the "/etc/networkd-dispatcher" base directory.	https://www.microsoft.com/security/blog/2022/04/26/microsoft-finds-new-elevation-of-privilege-linux-vulnerability-nimbuspwn/	A-MIC-WIND-101022/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29799		
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	6.1	Code Injection in GitHub repository microweber/microweber prior to 1.3.2. **CVE ID : CVE-2022-3242**	https://huntr.dev/bounties/3e6b218a-a5a6-40d9-9f7e-5ab0c6214faf, https://github.com/microweber/microweber/commit/68f0721571653db865a5fa01c7986642c82e919c	A-MIC-MICR-101022/941
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	6.1	HTML injection attack is closely related to Cross-site Scripting (XSS). HTML injection uses HTML to deface the page. XSS, as the name implies, injects JavaScript into the page. Both attacks exploit insufficient validation of user input. **CVE ID : CVE-2022-3245**	https://github.com/microweber/microweber/commit/f20abf30a1d9c1426c5fb757ac63998dc5b92bfc, https://huntr.dev/bounties/747c2924-95ca-4311-9e69-58ee0fb440a0	A-MIC-MICR-101022/942
Vendor: mobileeventsmanager					
Product: mobile_events_manager					
Affected Version(s): * Up to (excluding) 1.4.8					
Improper Neutralization of Formula	16-Sep-2022	8.8	The Mobile Events Manager WordPress plugin before 1.4.8 does	N/A	A-MOB-MOBI-101022/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in a CSV File			not properly escape the Enquiry source field when exporting events, or the Paid for field when exporting transactions as CSV, leading to a CSV injection vulnerability. **CVE ID : CVE-2022-1194**		
Vendor: moderncampus					
Product: omni_cms					
Affected Version(s): 10.2.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Sep-2022	9.8	Modern Campus Omni CMS (formerly OU Campus) 10.2.4 allows login-page SQL injection via a '" OR 1 = 1 -- - , <?php' substring. **CVE ID : CVE-2022-40766**	https://moderncampus.com/products/web-content-management.html	A-MOD-OMNI-101022/944
Vendor: msi					
Product: center					
Affected Version(s): 1.0.50.0					
N/A	19-Sep-2022	7.8	Micro-Star International Co., Ltd MSI Center 1.0.50.0 was discovered to contain a vulnerability in the component C_Features of MSI.CentralServer.exe. This vulnerability allows attackers to	N/A	A-MSI-CENT-101022/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges via running a crafted executable. **CVE ID : CVE-2022-38532**		
Vendor: mygraph_project					
Product: mygraph					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Sep-2022	5.4	MyGraph is a permission management system. Versions prior to 1.0.4 are vulnerable to a storage XSS vulnerability leading to Remote Code Execution. This issue is patched in version 1.0.4. There is no known workaround. **CVE ID : CVE-2022-39240**	https://github.com/renlm/MyGraph/security/advisories/GHSA-hj4j-923h-927j	A-MYG-MYGR-101022/946
Vendor: mz-automation					
Product: libiec61850					
Affected Version(s): * Up to (excluding) 1.5.0					
Out-of-bounds Write	23-Sep-2022	9.8	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) does not sanitize input before memcpy is used, which could allow an attacker to crash the device	N/A	A-MZ--LIBI-101022/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or remotely execute arbitrary code. **CVE ID : CVE-2022-2970**		
Out-of-bounds Write	23-Sep-2022	9.8	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) is vulnerable to a stack-based buffer overflow, which could allow an attacker to crash the device or remotely execute arbitrary code. **CVE ID : CVE-2022-2972**	N/A	A-MZ--LIBI-101022/948
Access of Resource Using Incompatible Type ('Type Confusion')	23-Sep-2022	7.5	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) accesses a resource using an incompatible type, which could allow an attacker to crash the server with a malicious payload. **CVE ID : CVE-2022-2971**	N/A	A-MZ--LIBI-101022/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	23-Sep-2022	7.5	MZ Automation's libIEC61850 (versions 1.4 and prior; version 1.5 prior to commit a3b04b7bc4872a5a39e5de3fdc5fbde52c09e10e) uses a NULL pointer in certain situations. which could allow an attacker to crash the server. **CVE ID : CVE-2022-2973**	N/A	A-MZ--LIBI-101022/950
Vendor: necta					
Product: wifi_mouse_server					
Affected Version(s): 1.7.8.5					
Improper Authentication	19-Sep-2022	9.8	Due to a reliance on client-side authentication, the WiFi Mouse (Mouse Server) from Necta LLC's authentication mechanism is trivially bypassed, which can result in remote code execution. **CVE ID : CVE-2022-3218**	https://github.com/rapid7/metasploit-framework/pull/16985	A-NEC-WIFI-101022/951
Vendor: nepxion					
Product: discovery					
Affected Version(s): * Up to (including) 6.16.2					
Improper Neutralization of Special Elements used in an	24-Sep-2022	9.8	Nepxion Discovery is a solution for Spring Cloud. Discover is vulnerable to SpEL Injection in	N/A	A-NEP-DISC-101022/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Expression Language Statement ('Expression Language Injection')			discovery-commons. DiscoveryExpressionResolver's eval method is evaluating expression with a StandardEvaluationContext, allowing the expression to reach and interact with Java classes such as java.lang.Runtime, leading to Remote Code Execution. There is no patch available for this issue at time of publication. There are no known workarounds. **CVE ID : CVE-2022-23463**		
Server-Side Request Forgery (SSRF)	24-Sep-2022	7.5	Nepxion Discovery is a solution for Spring Cloud. Discovery is vulnerable to a potential Server-Side Request Forgery (SSRF). RouterResourceImpl uses RestTemplate's getForEntity to retrieve the contents of a URL containing user-controlled input, potentially resulting in Information	N/A	A-NEP-DISC-101022/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure. There is no patch available for this issue at time of publication. There are no known workarounds. **CVE ID : CVE-2022-23464**		
Vendor: netic					
Product: group_export					
Affected Version(s): * Up to (excluding) 1.0.3					
Missing Authorization	17-Sep-2022	5.3	The Netic Group Export add-on before 1.0.3 for Atlassian Jira does not perform authorization checks. This might allow an unauthenticated user to export all groups from the Jira instance by making a groupexport_download=true request to a plugins/servlet/groupexportforjira/admin/ URI. **CVE ID : CVE-2022-39960**	https://marketplace.atlassian.com/apps/1222388/group-export-for-jira/version-history	A-NET-GROU-101022/954
Vendor: next-auth					
Product: nextauth					
Affected Version(s): * Up to (excluding) 3.0.2					
Improper Authentication	28-Sep-2022	8.1	`@next-auth/upstash-redis-adapter` is the Upstash Redis adapter for	https://github.com/nextauthjs/next-auth/security/advisories/GHSA	A-NEX-NEXT-101022/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NextAuth.js, which provides authentication for Next.js. Applications that use `next-auth` Email Provider and `@next-auth/upstash-redis-adapter` before v3.0.2 are affected by this vulnerability. The Upstash Redis adapter implementation did not check for both the identifier (email) and the token, but only checking for the identifier when verifying the token in the email callback flow. An attacker who knows about the victim's email could easily sign in as the victim, given the attacker also knows about the verification token's expired duration. The vulnerability is patched in v3.0.2. A workaround is available. Using Advanced Initialization, developers can check the requests and compare the query's token and	-4rxr-27mm-mxq9, https://github.com/nextauthjs/next-auth/commit/d16e04848ee703cf797724194d4ad2907fe125a9	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier before proceeding. **CVE ID : CVE-2022-39263**		
Vendor: Nextcloud					
Product: nextcloud					
Affected Version(s): * Up to (excluding) 3.21.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Sep-2022	5.5	Nextcloud android is the official Android client for the Nextcloud home server platform. Internal paths to the Nextcloud Android app files are not properly protected. As a result access to internal files of the from within the Nextcloud Android app is possible. This may lead to a leak of sensitive information in some cases. It is recommended that the Nextcloud Android app is upgraded to 3.21.0. There are no known workarounds for this issue. **CVE ID : CVE-2022-39210**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-vw2w-gpcv-v39f, https://github.com/nextcloud/android/pull/10544	A-NEX-NEXT-101022/956
Product: nextcloud_enterprise_server					
Affected Version(s): * Up to (excluding) 22.2.10.4					
Server-Side Request	16-Sep-2022	5.3	Nextcloud server is an open source personal cloud	https://github.com/nextcloud/server/pull/329	A-NEX-NEXT-101022/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			platform. In affected versions it was found that locally running webservices can be found and requested erroneously. It is recommended that the Nextcloud Server is upgraded to 23.0.8 or 24.0.4. It is recommended that the Nextcloud Enterprise Server is upgraded to 22.2.10.4, 23.0.8 or 24.0.4. There are no known workarounds for this issue. **CVE ID : CVE-2022-39211**	88, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-rmf9-w497-8cq8, https://github.com/nextcloud/server/pull/33031	
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.8					
Server-Side Request Forgery (SSRF)	16-Sep-2022	5.3	Nextcloud server is an open source personal cloud platform. In affected versions it was found that locally running webservices can be found and requested erroneously. It is recommended that the Nextcloud Server is upgraded to 23.0.8 or 24.0.4. It is recommended that the Nextcloud Enterprise Server is upgraded to	https://github.com/nextcloud/server/pull/32988, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-rmf9-w497-8cq8, https://github.com/nextcloud/server/pull/33031	A-NEX-NEXT-101022/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2.10.4, 23.0.8 or 24.0.4. There are no known workarounds for this issue. **CVE ID : CVE-2022-39211**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.4					
Server-Side Request Forgery (SSRF)	16-Sep-2022	5.3	Nextcloud server is an open source personal cloud platform. In affected versions it was found that locally running webservices can be found and requested erroneously. It is recommended that the Nextcloud Server is upgraded to 23.0.8 or 24.0.4. It is recommended that the Nextcloud Enterprise Server is upgraded to 22.2.10.4, 23.0.8 or 24.0.4. There are no known workarounds for this issue. **CVE ID : CVE-2022-39211**	https://github.com/nextcloud/server/pull/32988, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-rmf9-w497-8cq8, https://github.com/nextcloud/server/pull/33031	A-NEX-NEXT-101022/959
Product: nextcloud_server					
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.4					
Server-Side Request Forgery (SSRF)	16-Sep-2022	5.3	Nextcloud server is an open source personal cloud platform. In affected versions it was found that	https://github.com/nextcloud/server/pull/32988, https://github.com/nextcloud/s	A-NEX-NEXT-101022/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			locally running webservices can be found and requested erroneously. It is recommended that the Nextcloud Server is upgraded to 23.0.8 or 24.0.4. It is recommended that the Nextcloud Enterprise Server is upgraded to 22.2.10.4, 23.0.8 or 24.0.4. There are no known workarounds for this issue. **CVE ID : CVE-2022-39211**	ecurity-advisories/security/advisories/GHSA-rmf9-w497-8cq8, https://github.com/nextcloud/server/pull/33031	
Affected Version(s): * Up to (excluding) 23.0.8					
Server-Side Request Forgery (SSRF)	16-Sep-2022	5.3	Nextcloud server is an open source personal cloud platform. In affected versions it was found that locally running webservices can be found and requested erroneously. It is recommended that the Nextcloud Server is upgraded to 23.0.8 or 24.0.4. It is recommended that the Nextcloud Enterprise Server is upgraded to 22.2.10.4, 23.0.8 or 24.0.4. There are no known	https://github.com/nextcloud/server/pull/32988, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-rmf9-w497-8cq8, https://github.com/nextcloud/server/pull/33031	A-NEX-NEXT-101022/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-39211**		
Product: talk					
Affected Version(s): * Up to (excluding) 13.0.8					
N/A	17-Sep-2022	5.3	Nextcloud Talk is an open source chat, video & audio calls client for the Nextcloud platform. In affected versions an attacker could see the last video frame of any participant who has video disabled but a camera selected. It is recommended that the Nextcloud Talk app is upgraded to 13.0.8 or 14.0.4. Users unable to upgrade should select "None" as camera before joining the call. **CVE ID : CVE-2022-39212**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wq3g-2x46-q2gv, https://github.com/nextcloud/spreed/pull/7673	A-NEX-TALK-101022/962
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.0.4					
N/A	17-Sep-2022	5.3	Nextcloud Talk is an open source chat, video & audio calls client for the Nextcloud platform. In affected versions an attacker could see the last video frame of any	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-wq3g-2x46-q2gv, https://github.com/nextcloud/s	A-NEX-TALK-101022/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			participant who has video disabled but a camera selected. It is recommended that the Nextcloud Talk app is upgraded to 13.0.8 or 14.0.4. Users unable to upgrade should select "None" as camera before joining the call. **CVE ID : CVE-2022-39212**	preed/pull/7673	
Vendor: nheko_project					
Product: nheko					
Affected Version(s): * Up to (excluding) 0.10.2					
Improper Authentication	28-Sep-2022	5.9	nheko is a desktop client for the Matrix communication application. All versions below 0.10.2 are vulnerable homeservers inserting malicious secrets, which could lead to man-in-the-middle attacks. Users can upgrade to version 0.10.2 to protect against this issue. As a workaround, one may apply the patch manually, avoid doing verifications of one's own devices, and/or avoid	https://github.com/Nheko-Reborn/nheko/security/advisories/GHSA-8jcp-8jq4-5mm7, https://github.com/Nheko-Reborn/nheko/commit/67bee15a389f9b8a9f6c3a340558d1e2319e7199	A-NHE-NHEK-101022/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pressing the request button in the settings menu. **CVE ID : CVE-2022-39264**		
Vendor: nhn					
Product: toast_ui_grid					
Affected Version(s): * Up to (excluding) 4.21.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	Toast UI Grid is a component to display and edit data. Versions prior to 4.21.3 are vulnerable to cross-site scripting attacks when pasting specially crafted content into editable cells. This issue was fixed in version 4.21.3. There are no known workarounds. **CVE ID : CVE-2022-23458**	https://securitylab.github.com/advisories/GHSL-2022-029_nhn_tui_grid/, https://github.com/nhn/tui.grid/commit/e9db5968675ae113c07efc091cce210f2b26854f	A-NHN-TOAS-101022/965
Vendor: NI					
Product: configuration_manager					
Affected Version(s): * Up to (excluding) 22.5.0					
Improper Input Validation	16-Sep-2022	7.8	An improper input validation in NI System Configuration Manager before 22.5 may allow a privileged user to potentially enable escalation of privilege via local access.	https://ni.com, https://www.ni.com/en-us/support/documentation/supplemental/22/privilege-escalation-in-ni-configuration-manager-.html	A-NI-CONF-101022/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35415		
Vendor: nic					
Product: knot_resolver					
Affected Version(s): * Up to (excluding) 5.5.3					
Uncontrolled Resource Consumption	23-Sep-2022	7.5	Knot Resolver before 5.5.3 allows remote attackers to cause a denial of service (CPU consumption) because of algorithmic complexity. During an attack, an authoritative server must return large NS sets or address sets. **CVE ID : CVE-2022-40188**	https://gitlab.nic.cz/knot/knot-resolver/-/merge_requests/1343#note_262558	A-NIC-KNOT-101022/967
Vendor: Ninjaforms					
Product: ninja_forms					
Affected Version(s): * Up to (excluding) 3.6.13					
Deserialization of Untrusted Data	26-Sep-2022	7.2	The Ninja Forms Contact Form WordPress plugin before 3.6.13 unserialises the content of an imported file, which could lead to PHP object injections issues when an admin import (intentionally or not) a malicious file and a suitable gadget chain is	https://wpscan.com/vulnerability/255b98ba-5da9-4424-a7e9-c438d8905864	A-NIN-NINJ-101022/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present on the blog. **CVE ID : CVE-2022-2903**		
Vendor: Nlnetlabs					
Product: unbound					
Affected Version(s): * Up to (including) 1.16.2					
Uncontrolled Resource Consumption	26-Sep-2022	7.5	A vulnerability named 'Non-Responsive Delegation Attack' (NRDelegation Attack) has been discovered in various DNS resolving software. The NRDelegation Attack works by having a malicious delegation with a considerable number of non responsive nameservers. The attack starts by querying a resolver for a record that relies on those unresponsive nameservers. The attack can cause a resolver to spend a lot of time/resources resolving records under a malicious delegation point where a considerable number of unresponsive NS records reside. It	https://www.nlnetlabs.nl/downloads/unbound/CVE-2022-3204.txt	A-NLN-UNBO-101022/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trigger high CPU usage in some resolver implementations that continually look in the cache for resolved NS records in that delegation. This can lead to degraded performance and eventually denial of service in orchestrated attacks. Unbound does not suffer from high CPU usage, but resources are still needed for resolving the malicious delegation. Unbound will keep trying to resolve the record until hard limits are reached. Based on the nature of the attack and the replies, different limits could be reached. From version 1.16.3 on, Unbound introduces fixes for better performance when under load, by cutting opportunistic queries for nameserver discovery and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DNSKEY prefetching and limiting the number of times a delegation point can issue a cache lookup for missing records. **CVE ID : CVE-2022-3204**		
Vendor: Nokia					
Product: 1350_optical_management_system					
Affected Version(s): 14.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Sep-2022	6.5	An issue was discovered in NOKIA 1350OMS R14.2. Multiple Relative Path Traversal issues exist in different specific endpoints via the file parameter, allowing a remote authenticated attacker to read files on the filesystem arbitrarily. **CVE ID : CVE-2022-40713**	N/A	A-NOK-1350-101022/970
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Sep-2022	6.5	An issue was discovered in NOKIA 1350OMS R14.2. An Absolute Path Traversal vulnerability exists for a specific endpoint via the logfile parameter, allowing a remote authenticated	N/A	A-NOK-1350-101022/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to read files on the filesystem arbitrarily. **CVE ID : CVE-2022-40715**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	6.1	An issue was discovered in NOKIA 1350OMS R14.2. Reflected XSS exists under different /cgi-bin/R14.2* endpoints. **CVE ID : CVE-2022-40712**	N/A	A-NOK-1350-101022/972
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	6.1	An issue was discovered in NOKIA 1350OMS R14.2. Reflected XSS exists under different /oms1350/* endpoints. **CVE ID : CVE-2022-40714**	N/A	A-NOK-1350-101022/973
Vendor: notepad-plus-plus					
Product: notepad\+\+					
Affected Version(s): From (including) 8.3 Up to (excluding) 8.4.5					
Uncontrolled Search Path Element	28-Sep-2022	7.8	Notepad++ versions 8.4.1 and before are vulnerable to DLL hijacking where an attacker can replace the vulnerable dll (UxTheme.dll) with his own dll and run arbitrary code in	https://github.com/notepad-plus-plus/notepad-plus-plus/commit/85d7215d9b3e0d5a8433fc31aec4f2966821051e	A-NOT-NOTE-101022/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the context of Notepad++. **CVE ID : CVE-2022-32168**		
Vendor: notice_board_project					
Product: notice_board					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in NOTICE BOARD plugin <= 1.1 at WordPress. **CVE ID : CVE-2022-38460**	https://patchstack.com/database/vulnerability/notice-board/wordpress-notice-board-plugin-1-1-authenticated-stored-cross-site-scripting-xss-vulnerability/_s_id=cve, https://wordpress.org/plugins/notice-board/	A-NOT-NOTI-101022/975
Vendor: nuprocess_project					
Product: nuprocess					
Affected Version(s): From (including) 1.2.0 Up to (excluding) 2.0.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Sep-2022	9.8	NuProcess is an external process execution implementation for Java. In all the versions of NuProcess where it forks processes by using the JVM's Java_java_lang_UNIXProcess_forkAndExec method (1.2.0+), attackers can use NUL	https://github.com/brettwoldridge/NuProcess/commit/29bc09de561bf00ff9bf77123756363a9709f868, https://github.com/brettwoldridge/NuProcess/security/advisories/GHSA-cxgf-v2p8-7ph7, https://github.c	A-NUP-NUPR-101022/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			characters in their strings to perform command line injection. Java's ProcessBuilder isn't vulnerable because of a check in ProcessBuilder.start. NuProcess is missing that check. This vulnerability can only be exploited to inject command line arguments on Linux. Version 2.0.5 contains a patch. As a workaround, users of the library can sanitize command strings to remove NUL characters prior to passing them to NuProcess for execution. **CVE ID : CVE-2022-39243**	om/brettwoodridge/NuProcess/pull/143	
Vendor: nuxtjs					
Product: netlify-ipx					
Affected Version(s): * Up to (excluding) 1.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	netlify-ipx is an on-Demand image optimization for Netlify using ipx. In versions prior to 1.2.3, an attacker can bypass the source image domain allowlist by sending specially	https://github.com/netlify/netlify-ipx/security/advisories/GHSA-9jjv-524m-jm98	A-NUX-NETL-101022/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted headers, causing the handler to load and return arbitrary images. Because the response is cached globally, this image will then be served to visitors without requiring those headers to be set. XSS can be achieved by requesting a malicious SVG with embedded scripts, which would then be served from the site domain. Note that this does not apply to images loaded in `<img>` tags, as scripts do not execute in this context. The image URL can be set in the header independently of the request URL, meaning any site images that have not previously been cached can have their cache poisoned. This problem has been fixed in version 1.2.3. As a workaround, cached content can be cleared by re-deploying the site.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39239		
Vendor: oauth_client_single_sign_on_project					
Product: oauth_client_single_sign_on					
Affected Version(s): * Up to (excluding) 3.0.4					
Improper Authentication	26-Sep-2022	7.5	The OAuth client Single Sign On WordPress plugin before 3.0.4 does not have authorisation and CSRF when updating its settings, which could allow unauthenticated attackers to update them and change the OAuth endpoints to ones they controls, allowing them to then be authenticated as admin if they know the correct email address **CVE ID : CVE-2022-3119**	N/A	A-OAU-OAUT-101022/978
Vendor: octoprint					
Product: octoprint					
Affected Version(s): * Up to (excluding) 1.8.3					
Improper Privilege Management	21-Sep-2022	8.8	Improper Privilege Management in GitHub repository octoprint/octoprint prior to 1.8.3. **CVE ID : CVE-2022-3068**	https://huntr.dev/bounties/f45c24cb-9104-4c6e-a9e1-5c7e75e83884, https://github.com/octoprint/octoprint/commit/ef95ef1c101b	A-OCT-OCTO-101022/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				79394f134e8fce000e6bae046571	
Unrestricted Upload of File with Dangerous Type	21-Sep-2022	5.4	Unrestricted Upload of File with Dangerous Type in GitHub repository octoprint/octoprint prior to 1.8.3. **CVE ID : CVE-2022-2872**	https://github.com/octoprint/octoprint/commit/3e3c11811e216fb371a33e28412df83f9701e5b0, https://huntr.dev/bounties/b966c74d-6f3f-49fe-b40a-eaf25e362c56	A-OCT-OCTO-101022/980
Insufficient Session Expiration	21-Sep-2022	4.4	If an attacker comes into the possession of a victim's OctoPrint session cookie through whatever means, the attacker can use this cookie to authenticate as long as the victim's account exists. **CVE ID : CVE-2022-2888**	https://github.com/octoprint/octoprint/commit/40e6217ac1a85cc5ed592873ae49db01d3005da4, https://huntr.dev/bounties/d27d232b-2578-4b32-b3b4-74aabdadf629	A-OCT-OCTO-101022/981
Vendor: octopus					
Product: octopus_server					
Affected Version(s): From (including) 2019.5.7 Up to (excluding) 2022.1.3180					
Generation of Error Message Containing Sensitive Information	28-Sep-2022	4.3	In affected versions of Octopus Deploy it is possible to reveal the Space ID of spaces that the user does not have access to view in an error message when a resource is	https://advisories.octopus.com/post/2022/sa2022-14/	A-OCT-OCTO-101022/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			part of another Space. **CVE ID : CVE-2022-2760**		
Affected Version(s): From (including) 2022.2.0 Up to (excluding) 2022.2.7965					
Generation of Error Message Containing Sensitive Information	28-Sep-2022	4.3	In affected versions of Octopus Deploy it is possible to reveal the Space ID of spaces that the user does not have access to view in an error message when a resource is part of another Space. **CVE ID : CVE-2022-2760**	https://advisories.octopus.com/post/2022/sa2022-14/	A-OCT-OCTO-101022/983
Affected Version(s): From (including) 2022.3.0 Up to (excluding) 2022.3.10405					
Generation of Error Message Containing Sensitive Information	28-Sep-2022	4.3	In affected versions of Octopus Deploy it is possible to reveal the Space ID of spaces that the user does not have access to view in an error message when a resource is part of another Space. **CVE ID : CVE-2022-2760**	https://advisories.octopus.com/post/2022/sa2022-14/	A-OCT-OCTO-101022/984
Vendor: online_banking_system_project					
Product: online_banking_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection	N/A	A-ONL-ONLI-101022/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			vulnerability via the cust_id parameter at /net-banking/send_funds.php. **CVE ID : CVE-2022-40113**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/edit_customer.php. **CVE ID : CVE-2022-40114**	N/A	A-ONL-ONLI-101022/986
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/delete_beneficiary.php. **CVE ID : CVE-2022-40115**	N/A	A-ONL-ONLI-101022/987
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search parameter at /net-banking/beneficiary.php.	N/A	A-ONL-ONLI-101022/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40116		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/delete_customer.php. **CVE ID : CVE-2022-40117**	N/A	A-ONL-ONLI-101022/989
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/send_funds_action.php. **CVE ID : CVE-2022-40118**	N/A	A-ONL-ONLI-101022/990
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search_term parameter at /net-banking/transactions.php. **CVE ID : CVE-2022-40119**	N/A	A-ONL-ONLI-101022/991
Improper Neutralization of Special	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL	N/A	A-ONL-ONLI-101022/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			injection vulnerability via the search_term parameter at /net-banking/customer_transactions.php. **CVE ID : CVE-2022-40120**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the search parameter at /net-banking/manage_customers.php. **CVE ID : CVE-2022-40121**	N/A	A-ONL-ONLI-101022/993
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	9.8	Online Banking System v1.0 was discovered to contain a SQL injection vulnerability via the cust_id parameter at /net-banking/edit_customer_action.php. **CVE ID : CVE-2022-40122**	N/A	A-ONL-ONLI-101022/994
Vendor: online_leave_management_system_project					
Product: online_leave_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	26-Sep-2022	7.2	Online Leave Management System v1.0 is vulnerable to SQL Injection via /leave_system/clas	N/A	A-ONL-ONLI-101022/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			ses/Master.php?f=delete_leave_type. **CVE ID : CVE-2022-40926**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	7.2	Online Leave Management System v1.0 is vulnerable to SQL Injection via /leave_system/classes/Master.php?f=delete_designation. **CVE ID : CVE-2022-40927**	N/A	A-ONL-ONLI-101022/996
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	7.2	Online Leave Management System v1.0 is vulnerable to SQL Injection via /leave_system/classes/Master.php?f=delete_application. **CVE ID : CVE-2022-40928**	N/A	A-ONL-ONLI-101022/997
Vendor: online_market_place_site_project					
Product: online_market_place_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	9.8	Sourcecodester Online Market Place Site v1.0 suffers from an unauthenticated blind SQL Injection Vulnerability allowing remote attackers to dump the SQL database via time-based SQL injection..	N/A	A-ONL-ONLI-101022/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30004		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	5.4	Sourcecodester Online Market Place Site 1.0 is vulnerable to Cross Site Scripting (XSS), allowing attackers to register as a Seller then create new products containing XSS payloads in the 'Product Title' and 'Short Description' fields. **CVE ID : CVE-2022-30003**	N/A	A-ONL-ONLI-101022/999
Vendor: online_pet_shop_web_application_project					
Product: online_pet_shop_web_application					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Sep-2022	7.2	Online Pet Shop We App v1.0 by oretnom23 is vulnerable to SQL injection via /pet_shop/classes/Master.php?f=delete_order,id. **CVE ID : CVE-2022-40933**	N/A	A-ONL-ONLI-101022/1000
Improper Neutralization of Special Elements used in an SQL Command	22-Sep-2022	7.2	Online Pet Shop We App v1.0 is vulnerable to SQL injection via /pet_shop/classes/Master.php?f=delete_sub_category,id **CVE ID : CVE-2022-40934**	N/A	A-ONL-ONLI-101022/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Sep-2022	7.2	Online Pet Shop We App v1.0 is vulnerable to SQL Injection via /pet_shop/classes/Master.php?f=delete_category,id. **CVE ID : CVE-2022-40935**	N/A	A-ONL-ONLI-101022/1002
Vendor: online_tours_and_travels_management_system_project					
Product: online_tours_and_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tour/admin/update_packages.php. **CVE ID : CVE-2022-40091**	N/A	A-ONL-ONLI-101022/1003
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tour/admin/update_payment.php. **CVE ID : CVE-2022-40092**	N/A	A-ONL-ONLI-101022/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /tour/admin/update_tax.php. **CVE ID : CVE-2022-40093**	N/A	A-ONL-ONLI-101022/1005
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_currency.php. **CVE ID : CVE-2022-40097**	N/A	A-ONL-ONLI-101022/1006
Vendor: online_tours_\&_travels_management_system					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_traveller.php.	N/A	A-ONL-ONLI-101022/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40352		
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_expense.php. **CVE ID : CVE-2022-40098**	N/A	A-ONL-ONLI-101022/1008
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_expense_category.php. **CVE ID : CVE-2022-40099**	N/A	A-ONL-ONLI-101022/1009
Improper Neutralization of Special Elements used in an SQL Command	27-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at	N/A	A-ONL-ONLI-101022/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			/admin/up_booking.php. **CVE ID : CVE-2022-40353**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-2022	7.2	Online Tours & Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/update_booking.php. **CVE ID : CVE-2022-40354**	N/A	A-ONL-ONLI-101022/1011
Vendor: open5gs					
Product: open5gs					
Affected Version(s): * Up to (including) 2.4.10					
Improper Resource Shutdown or Release	28-Sep-2022	7.5	A vulnerability has been found in Open5GS up to 2.4.10 and classified as problematic. This vulnerability affects unknown code in the library lib/core/ogs-tlv-msg.c of the component UDP Packet Handler. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-	N/A	A-OPE-OPEN-101022/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			209686 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3354**		
Affected Version(s): * Up to (including) 2.4.9					
N/A	16-Sep-2022	7.5	When Open5GS UPF receives a PFCP Session Establishment Request, it stores related values for building the PFCP Session Establishment Response. Once UPF receives a request, it gets the f_teid_len from incoming message, and then uses it to copy data from incoming message to struct f_teid without checking the maximum length. If the pdi.local_f_teid.len exceeds the maximum length of the struct of f_teid, the memcpy() overwrites the fields (e.g., f_teid_len) after f_teid in the pdr struct. After parsing the request, the UPF starts to build a response. The f_teid_len with its	N/A	A-OPE-OPEN-101022/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overwritten value is used as a length for memcpy(). A segmentation fault occurs, as a result of a memcpy(), if this overwritten value is large enough. **CVE ID : CVE-2022-39063**		
Vendor: openwrt					
Product: openwrt					
Affected Version(s): * Up to (excluding) 21.02.3					
N/A	19-Sep-2022	7.5	Openwrt before v21.02.3 and Openwrt v22.03.0-rc6 were discovered to contain two skip loops in the function header_value(). This vulnerability allows attackers to access sensitive information via a crafted HTTP request. **CVE ID : CVE-2022-38333**	https://git.openwrt.org/?p=project/cgi-io.git;a=commitdiff;h=901b0f0463c9d16a8cf5b9ed37118d8484bc9176, https://git.openwrt.org/?p=project/cgi-io.git;a=commit;h=901b0f0463c9d16a8cf5b9ed37118d8484bc9176	A-OPE-OPEN-101022/1014
Affected Version(s): 22.03.0					
N/A	19-Sep-2022	7.5	Openwrt before v21.02.3 and Openwrt v22.03.0-rc6 were discovered to contain two skip loops in the function header_value().	https://git.openwrt.org/?p=project/cgi-io.git;a=commitdiff;h=901b0f0463c9d16a8cf5b9ed37118d8484bc9176, https://git.open	A-OPE-OPEN-101022/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability allows attackers to access sensitive information via a crafted HTTP request. **CVE ID : CVE-2022-38333**	wrt.org/?p=project/cgi-io.git;a=commit;h=901b0f0463c9d16a8cf5b9ed37118d8484bc9176	
Vendor: opswat					
Product: metadefender					
Affected Version(s): * Up to (excluding) 4.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	5.4	A stored Cross-Site Scripting (XSS) vulnerability in OPSWAT MetaDefender ICAP Server before 4.13.0 allows attackers to execute arbitrary JavaScript or HTML because of the blocked page response. **CVE ID : CVE-2022-40778**	https://www.opswat.com/products/metadefender/icap, https://docs.opswat.com/mdicap/release-notes	A-OPS-META-101022/1016
Vendor: orckestra					
Product: c1_cms					
Affected Version(s): * Up to (excluding) 6.13					
Deserialization of Untrusted Data	27-Sep-2022	8	Orckestra C1 CMS is a .NET based Web Content Management System. A vulnerability in versions prior to 6.13 allows remote attackers to execute arbitrary code on affected installations of	https://github.com/Orckestra/C1-CMS-Foundation/pull/814, https://github.com/Orckestra/C1-CMS-Foundation/security/advisories	A-ORC-C1_C-101022/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Orckestra C1 CMS. Authentication is required to exploit this vulnerability. The authenticated user may perform the actions unknowingly by visiting a specially crafted site. This issue is patched in C1 CMS v6.13. There are no known workarounds. **CVE ID : CVE-2022-39256**	/GHSA-gfhp-jgp6-838j	
Vendor: otfcc_project					
Product: otfcc					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a global buffer overflow via /release-x64/otfccdump+0x718693. **CVE ID : CVE-2022-35021**	N/A	A-OTF-OTFC-101022/1018
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6badae. **CVE ID : CVE-2022-35022**	N/A	A-OTF-OTFC-101022/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /lib/x86_64-linux-gnu/libc.so.6+0xbb384. **CVE ID : CVE-2022-35023**	N/A	A-OTF-OTFC-101022/1020
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /multiarch/memmove-vec-unaligned-erms.S. **CVE ID : CVE-2022-35024**	N/A	A-OTF-OTFC-101022/1021
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x5266a8. **CVE ID : CVE-2022-35025**	N/A	A-OTF-OTFC-101022/1022
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fbc0b.	N/A	A-OTF-OTFC-101022/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35026		
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fe9a7. **CVE ID : CVE-2022-35027**	N/A	A-OTF-OTFC-101022/1024
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fbbb6. **CVE ID : CVE-2022-35028**	N/A	A-OTF-OTFC-101022/1025
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6babea. **CVE ID : CVE-2022-35029**	N/A	A-OTF-OTFC-101022/1026
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-	N/A	A-OTF-OTFC-101022/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x64/otfccdump+0x4fe954. **CVE ID : CVE-2022-35030**		
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x703969. **CVE ID : CVE-2022-35031**	N/A	A-OTF-OTFC-101022/1028
N/A	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6b6a8f. **CVE ID : CVE-2022-35032**	N/A	A-OTF-OTFC-101022/1029
Out-of-bounds Write	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e7e3d. **CVE ID : CVE-2022-35034**	N/A	A-OTF-OTFC-101022/1030
Out-of-bounds Write	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via	N/A	A-OTF-OTFC-101022/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/release-x64/otfccdump+0x6b559f. **CVE ID : CVE-2022-35035**		
Out-of-bounds Write	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e1fc8. **CVE ID : CVE-2022-35036**	N/A	A-OTF-OTFC-101022/1032
Out-of-bounds Write	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6adb1e. **CVE ID : CVE-2022-35037**	N/A	A-OTF-OTFC-101022/1033
Out-of-bounds Write	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b064d. **CVE ID : CVE-2022-35038**	N/A	A-OTF-OTFC-101022/1034
Out-of-bounds Write	22-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-	N/A	A-OTF-OTFC-101022/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x64/otfccdump+0x6e20a0. **CVE ID : CVE-2022-35039**		
Affected Version(s): 2022-06-03					
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c0a32. **CVE ID : CVE-2022-35060**	N/A	A-OTF-OTFC-101022/1036
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e412a. **CVE ID : CVE-2022-35061**	N/A	A-OTF-OTFC-101022/1037
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6c0bc3. **CVE ID : CVE-2022-35062**	N/A	A-OTF-OTFC-101022/1038
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-	N/A	A-OTF-OTFC-101022/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x64/otfccdump+0x6e41a8. **CVE ID : CVE-2022-35063**		
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x4adcdb in __asan_memset. **CVE ID : CVE-2022-35064**	N/A	A-OTF-OTFC-101022/1040
N/A	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a segmentation violation via /release-x64/otfccdump+0x65f724. **CVE ID : CVE-2022-35065**	N/A	A-OTF-OTFC-101022/1041
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e41b8. **CVE ID : CVE-2022-35066**	N/A	A-OTF-OTFC-101022/1042
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via	N/A	A-OTF-OTFC-101022/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/release-x64/otfccdump+0x6e41b0. **CVE ID : CVE-2022-35067**		
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6e420d. **CVE ID : CVE-2022-35068**	N/A	A-OTF-OTFC-101022/1044
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x6b544e. **CVE ID : CVE-2022-35069**	N/A	A-OTF-OTFC-101022/1045
Out-of-bounds Write	19-Sep-2022	6.5	OTFCC commit 617837b was discovered to contain a heap buffer overflow via /release-x64/otfccdump+0x65fc97. **CVE ID : CVE-2022-35070**	N/A	A-OTF-OTFC-101022/1046
Vendor: Ovirt					
Product: ovirt-engine					
Affected Version(s): 4.3.0					
Improper Neutralizat	28-Sep-2022	6.1	An HTML injection/reflected	N/A	A-OVI-OVIR-101022/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Cross-site scripting (XSS) vulnerability was found in the ovirt-engine. A parameter "error_description" fails to sanitize the entry, allowing the vulnerability to trigger on the Windows Service Accounts home pages. **CVE ID : CVE-2022-3193**		
Vendor: Owasp					
Product: owasp_modsecurity_core_rule_set					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.2.2					
N/A	20-Sep-2022	9.8	The OWASP ModSecurity Core Rule Set (CRS) is affected by a partial rule set bypass by submitting a specially crafted HTTP Content-Type header field that indicates multiple character encoding schemes. A vulnerable back-end can potentially be exploited by declaring multiple Content-Type "charset" names and therefore bypassing the configurable CRS Content-Type header "charset"	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow list. An encoded payload can bypass CRS detection this way and may then be decoded by the backend. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised to upgrade to 3.2.2 and 3.3.3 respectively. **CVE ID : CVE-2022-39955**		
Improper Encoding or Escaping of Output	20-Sep-2022	9.8	The OWASP ModSecurity Core Rule Set (CRS) is affected by a partial rule set bypass for HTTP multipart requests by submitting a payload that uses a character encoding scheme via the Content-Type or the deprecated Content-Transfer-Encoding multipart MIME header fields that will not be decoded and inspected by the web application firewall engine and the rule set. The	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multipart payload will therefore bypass detection. A vulnerable backend that supports these encoding schemes can potentially be exploited. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised upgrade to 3.2.2 and 3.3.3 respectively. The mitigation against these vulnerabilities depends on the installation of the latest ModSecurity version (v2.9.6 / v3.0.8). **CVE ID : CVE-2022-39956**		
Improper Encoding or Escaping of Output	20-Sep-2022	7.5	The OWASP ModSecurity Core Rule Set (CRS) is affected by a response body bypass. A client can issue an HTTP Accept header field containing an optional "charset" parameter in order to receive the	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response in an encoded form. Depending on the "charset", this response can not be decoded by the web application firewall. A restricted resource, access to which would ordinarily be detected, may therefore bypass detection. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised to upgrade to 3.2.2 and 3.3.3 respectively. **CVE ID : CVE-2022-39957**		
Improper Encoding or Escaping of Output	20-Sep-2022	7.5	The OWASP ModSecurity Core Rule Set (CRS) is affected by a response body bypass to sequentially exfiltrate small and undetectable sections of data by repeatedly submitting an HTTP Range header field with a small byte range. A	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted resource, access to which would ordinarily be detected, may be exfiltrated from the backend, despite being protected by a web application firewall that uses CRS. Short subsections of a restricted resource may bypass pattern matching techniques and allow undetected access. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised to upgrade to 3.2.2 and 3.3.3 respectively and to configure a CRS paranoia level of 3 or higher. **CVE ID : CVE-2022-39958**		
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.3					
N/A	20-Sep-2022	9.8	The OWASP ModSecurity Core Rule Set (CRS) is affected by a partial rule set bypass by submitting a specially crafted	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTP Content-Type header field that indicates multiple character encoding schemes. A vulnerable back-end can potentially be exploited by declaring multiple Content-Type "charset" names and therefore bypassing the configurable CRS Content-Type header "charset" allow list. An encoded payload can bypass CRS detection this way and may then be decoded by the backend. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised to upgrade to 3.2.2 and 3.3.3 respectively. **CVE ID : CVE-2022-39955**		
Improper Encoding or Escaping of Output	20-Sep-2022	9.8	The OWASP ModSecurity Core Rule Set (CRS) is affected by a partial rule set bypass for HTTP	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-	A-OWA-OWAS-101022/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multipart requests by submitting a payload that uses a character encoding scheme via the Content-Type or the deprecated Content-Transfer-Encoding multipart MIME header fields that will not be decoded and inspected by the web application firewall engine and the rule set. The multipart payload will therefore bypass detection. A vulnerable backend that supports these encoding schemes can potentially be exploited. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised upgrade to 3.2.2 and 3.3.3 respectively. The mitigation against these vulnerabilities depends on the installation of the latest ModSecurity	covering-several-cves/	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version (v2.9.6 / v3.0.8). **CVE ID : CVE-2022-39956**		
Improper Encoding or Escaping of Output	20-Sep-2022	7.5	The OWASP ModSecurity Core Rule Set (CRS) is affected by a response body bypass. A client can issue an HTTP Accept header field containing an optional "charset" parameter in order to receive the response in an encoded form. Depending on the "charset", this response can not be decoded by the web application firewall. A restricted resource, access to which would ordinarily be detected, may therefore bypass detection. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised to upgrade to 3.2.2 and 3.3.3 respectively.	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39957		
Improper Encoding or Escaping of Output	20-Sep-2022	7.5	The OWASP ModSecurity Core Rule Set (CRS) is affected by a response body bypass to sequentially exfiltrate small and undetectable sections of data by repeatedly submitting an HTTP Range header field with a small byte range. A restricted resource, access to which would ordinarily be detected, may be exfiltrated from the backend, despite being protected by a web application firewall that uses CRS. Short subsections of a restricted resource may bypass pattern matching techniques and allow undetected access. The legacy CRS versions 3.0.x and 3.1.x are affected, as well as the currently supported versions 3.2.1 and 3.3.2. Integrators and users are advised to upgrade to 3.2.2	https://coreruleset.org/20220919/crs-version-3-3-3-and-3-2-2-covering-several-cves/	A-OWA-OWAS-101022/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 3.3.3 respectively and to configure a CRS paranoia level of 3 or higher. **CVE ID : CVE-2022-39958**		
Vendor: oxilab					
Product: image_hover_effects_ultimate					
Affected Version(s): * Up to (excluding) 9.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	The Image Hover Effects Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Title & Description values that can be added to an Image Hover in versions up to, and including, 9.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By default, the plugin only allows administrators access to edit Image Hovers, however, if a site	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2669411%40image-hover-effects-ultimate&new=2669411%40image-hover-effects-ultimate&sfp_email=&sfph_mail=	A-OXI-IMAG-101022/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin makes the plugin's features available to lower privileged users through the 'Who Can Edit?' setting then this can be exploited by those users. **CVE ID : CVE-2022-2937**		
Vendor: pagekit					
Product: pagekit					
Affected Version(s): 1.0.18					
Unrestricted Upload of File with Dangerous Type	20-Sep-2022	9.8	A file upload vulnerability exists in the storage feature of pagekit 1.0.18, which allows an attacker to upload malicious files **CVE ID : CVE-2022-38916**	N/A	A-PAG-PAGE-101022/1057
Vendor: parantezteknoloji					
Product: koha_library_automation					
Affected Version(s): * Up to (excluding) 19.05.03.01					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Sep-2022	9.8	The library automation system product KOHA developed by Parantez Teknoloji before version 19.05.03 has an unauthenticated SQL Injection vulnerability. This has been fixed in the version 19.05.03.01.	https://www.usom.gov.tr/bildirim/tr-22-0635	A-PAR-KOHA-101022/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0495		
Vendor: parity					
Product: frontier					
Affected Version(s): * Up to (excluding) 2022-09-12					
Incorrect Calculation	24-Sep-2022	5.3	Frontier is an Ethereum compatibility layer for Substrate. Prior to commit d3beddc6911a559a3ecc9b3f08e153dbe37a8658, the worst case weight was always accounted as the block weight for all cases. In case of large EVM gas refunds, this can lead to block spamming attacks -- the adversary can construct blocks with transactions that have large amount of refunds or unused gases with reverts, and as a result inflate up the chain gas prices. The impact of this issue is limited in that the spamming attack would still be costly for any adversary, and it has no ability to alter any chain state. This issue has been patched in commit	https://github.com/paritytech/frontier/pull/851, https://github.com/paritytech/frontier/security/advisories/GHSA-v57h-6hmh-g2p4	A-PAR-FRON-101022/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d3beddc6911a559a3ecc9b3f08e153dbe37a8658. There are no known workarounds. **CVE ID : CVE-2022-39242**		
Vendor: parseplatform					
Product: parse-server					
Affected Version(s): * Up to (excluding) 4.10.15					
Incorrect Resource Transfer Between Spheres	23-Sep-2022	3.1	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.15, or 5.0.0 and above prior to 5.2.6, a user can write to the session object of another user if the session object ID is known. For example, an attacker can assign the session object to their own user by writing to the `user` field and then read any custom fields of that session object. Note that assigning a session to another user does not usually change the privileges of either of the two users, and a user cannot assign their own session to	https://github.com/parse-community/parse-server/security/advisories/GHSA-6w4q-23cf-j9jp	A-PAR-PARS-101022/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			another user. This issue is patched in version 4.10.15 and above, and 5.2.6 and above. To mitigate this issue in unpatched versions add a `beforeSave` trigger to the `_Session` class and prevent writing if the requesting user is different from the user in the session object. **CVE ID : CVE-2022-39225**		
Affected Version(s): * Up to (excluding) 4.10.16					
Improper Authentication	23-Sep-2022	3.7	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.16, or from 5.0.0 to 5.2.6, validation of the authentication adapter app ID for _Facebook_ and _Spotify_ may be circumvented. Configurations which allow users to authenticate using the Parse Server authentication adapter where `appIds` is set as a string instead of an	https://github.com/parse-community/parse-server/security/advisories/GHSA-r657-33vp-gp22	A-PAR-PARS-101022/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			array of strings authenticate requests from an app with a different app ID than the one specified in the `appIds` configuration. For this vulnerability to be exploited, an attacker needs to be assigned an app ID by the authentication provider which is a sub-set of the server-side configured app ID. This issue is patched in versions 4.10.16 and 5.2.7. There are no known workarounds. **CVE ID : CVE-2022-39231**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.2.6					
Incorrect Resource Transfer Between Spheres	23-Sep-2022	3.1	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to 4.10.15, or 5.0.0 and above prior to 5.2.6, a user can write to the session object of another user if the session object ID is known. For example, an	https://github.com/parse-community/parse-server/security/advisories/GHSA-6w4q-23cf-j9jp	A-PAR-PARS-101022/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can assign the session object to their own user by writing to the `user` field and then read any custom fields of that session object. Note that assigning a session to another user does not usually change the privileges of either of the two users, and a user cannot assign their own session to another user. This issue is patched in version 4.10.15 and above, and 5.2.6 and above. To mitigate this issue in unpatched versions add a `beforeSave` trigger to the `_Session` class and prevent writing if the requesting user is different from the user in the session object. **CVE ID : CVE-2022-39225**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.2.7					
Improper Authentication	23-Sep-2022	3.7	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. In versions prior to	https://github.com/parse-community/parse-server/security/advisories/GH	A-PAR-PARS-101022/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.10.16, or from 5.0.0 to 5.2.6, validation of the authentication adapter app ID for _Facebook_ and _Spotify_ may be circumvented. Configurations which allow users to authenticate using the Parse Server authentication adapter where `appIds` is set as a string instead of an array of strings authenticate requests from an app with a different app ID than the one specified in the `appIds` configuration. For this vulnerability to be exploited, an attacker needs to be assigned an app ID by the authentication provider which is a sub-set of the server-side configured app ID. This issue is patched in versions 4.10.16 and 5.2.7. There are no known workarounds.	SA-r657-33vp-gp22	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39231		
Vendor: pbc_project					
Product: pbc					
Affected Version(s): * Up to (including) 2022-08-27					
Unchecked Return Value	23-Sep-2022	7.5	An issue has been found in PBC through 2022-8-27. A SEGV issue detected in the function pbc_wmessage_integer in src/wmessage.c:137. **CVE ID : CVE-2022-38936**	N/A	A-PBC-PBC-101022/1064
Vendor: pdssoftware					
Product: pds_vista_7					
Affected Version(s): * Up to (excluding) 7.1.7.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	6.5	The 'document' parameter of PDS Vista 7's /application/documents/display.aspx page is vulnerable to a Local File Inclusion vulnerability which allows an low-privileged authenticated attacker to leak the configuration files and source code of the web application. **CVE ID : CVE-2022-34002**	N/A	A-PDS-PDS_-101022/1065
Vendor: PHP					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: php					
Affected Version(s): * Up to (excluding) 7.4.31					
N/A	28-Sep-2022	6.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications. **CVE ID : CVE-2022-31629**	https://bugs.php.net/bug.php?id=81727	A-PHP-PHP-101022/1066
Uncontrolled Recursion	28-Sep-2022	5.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop. **CVE ID : CVE-2022-31628**	N/A	A-PHP-PHP-101022/1067
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.24					
N/A	28-Sep-2022	6.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the	https://bugs.php.net/bug.php?id=81727	A-PHP-PHP-101022/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications. **CVE ID : CVE-2022-31629**		
Uncontrolled Recursion	28-Sep-2022	5.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop. **CVE ID : CVE-2022-31628**	N/A	A-PHP-PHP-101022/1069
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.11					
N/A	28-Sep-2022	6.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications. **CVE ID : CVE-2022-31629**	https://bugs.php.net/bug.php?id=81727	A-PHP-PHP-101022/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Recursion	28-Sep-2022	5.5	In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop. **CVE ID : CVE-2022-31628**	N/A	A-PHP-PHP-101022/1071
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	4.8	If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user. Amongst other things, the attacker can: Perform any action within the application that the user can perform. View any information that the user is able to view. Modify any information that the user is able to modify. Initiate interactions with other application users, including malicious attacks, that will appear to	https://huntr.dev/bounties/0ea45cf9-b256-454c-9031-2435294c0902, https://github.com/pimcore/pimcore/commit/1e916e7d668c9e47b217e20cc0ea4812f466201b	A-PIM-PIMC-101022/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			originate from the initial victim user. **CVE ID : CVE-2022-3255**		
Vendor: postmansmtp					
Product: post_smtp_mailer\/email_log					
Affected Version(s): * Up to (excluding) 2.1.7					
Server-Side Request Forgery (SSRF)	26-Sep-2022	7.2	The Post SMTP Mailer/Email Log WordPress plugin before 2.1.7 does not have proper authorisation in some AJAX actions, which could allow high privilege users such as admin to perform blind SSRF on multisite installations for example. **CVE ID : CVE-2022-2352**	https://wpscan.com/vulnerability/dc99ac40-646a-4f8e-b2b9-dc55d6d4c55c	A-POS-POST-101022/1073
Vendor: processmaker					
Product: processmaker					
Affected Version(s): 3.5.4					
Improper Preservation of Permissions	19-Sep-2022	8.8	ProcessMaker before v3.5.4 was discovered to contain insecure permissions in the user profile page. This vulnerability allows attackers to escalate normal users to Administrators. **CVE ID : CVE-2022-38577**	N/A	A-PRO-PROC-101022/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: profanity_project					
Product: profanity					
Affected Version(s): * Up to (including) 1.60					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	18-Sep-2022	7.5	profanity through 1.60 has only four billion possible RNG initializations. Thus, attackers can recover private keys from Ethereum vanity addresses and steal cryptocurrency, as exploited in the wild in June 2022. **CVE ID : CVE-2022-40769**	N/A	A-PRO-PROF-101022/1075
Vendor: python-jwt_project					
Product: python-jwt					
Affected Version(s): * Up to (excluding) 3.3.4					
Authentication Bypass by Spoofing	23-Sep-2022	9.1	python-jwt is a module for generating and verifying JSON Web Tokens. Versions prior to 3.3.4 are subject to Authentication Bypass by Spoofing, resulting in identity spoofing, session hijacking or authentication bypass. An attacker who obtains a JWT can arbitrarily forge its contents without knowing the secret key. Depending on the	https://github.com/davedoesdev/python-jwt/commit/88ad9e67c53aa5f7c43ec4aa52ed34b7930068c9, https://github.com/davedoesdev/python-jwt/security/advisories/GHSA-5p8v-58qm-c7fp	A-PYT-PYTH-101022/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application, this may for example enable the attacker to spoof other user's identities, hijack their sessions, or bypass authentication. Users should upgrade to version 3.3.4. There are no known workarounds. **CVE ID : CVE-2022-39227**		
Vendor: quantumcloud					
Product: slider_hero					
Affected Version(s): * Up to (excluding) 8.4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	4.8	The Slider Hero WordPress plugin before 8.4.4 does not escape the slider Name, which could allow high-privileged users to perform Cross-Site Scripting attacks. **CVE ID : CVE-2022-3074**	https://wpscan.com/vulnerability/90ebaedc-89df-413f-b22e-753d4dd5e1c3	A-QUA-SLID-101022/1077
Vendor: radiustheme					
Product: classified_listing_-_classified_ads_\&_business_directory					
Affected Version(s): * Up to (excluding) 2.2.14					
Improper Neutralization of Input During Web Page Generation	16-Sep-2022	6.1	The Classima WordPress theme before 2.1.11 and some of its required plugins (Classified Listing before 2.2.14, Classified Listing Pro before 2.0.20,	N/A	A-RAD-CLAS-101022/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Classified Listing Store & Membership before 1.4.20 and Classima Core before 1.10) do not escape a parameter before outputting it back in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-2654**		
Product: classified_listing_pro_-_classified_ads_\&_business_directory					
Affected Version(s): * Up to (excluding) 2.0.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	6.1	The Classima WordPress theme before 2.1.11 and some of its required plugins (Classified Listing before 2.2.14, Classified Listing Pro before 2.0.20, Classified Listing Store & Membership before 1.4.20 and Classima Core before 1.10) do not escape a parameter before outputting it back in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-2654**	N/A	A-RAD-CLAS-101022/1079
Improper Neutralization of	16-Sep-2022	6.1	The Classified Listing Pro WordPress plugin	N/A	A-RAD-CLAS-101022/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			before 2.0.20 does not escape a generated URL before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-2655**		
Product: classified_listing_store_\&_membership					
Affected Version(s): * Up to (excluding) 1.4.20					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	6.1	The Classima WordPress theme before 2.1.11 and some of its required plugins (Classified Listing before 2.2.14, Classified Listing Pro before 2.0.20, Classified Listing Store & Membership before 1.4.20 and Classima Core before 1.10) do not escape a parameter before outputting it back in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-2654**	N/A	A-RAD-CLAS-101022/1081
Product: classima					
Affected Version(s): * Up to (excluding) 2.1.11					
Improper Neutralization of	16-Sep-2022	6.1	The Classima WordPress theme before 2.1.11 and	N/A	A-RAD-CLAS-101022/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			some of its required plugins (Classified Listing before 2.2.14, Classified Listing Pro before 2.0.20, Classified Listing Store & Membership before 1.4.20 and Classima Core before 1.10) do not escape a parameter before outputting it back in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-2654**		
Product: classima_core					
Affected Version(s): * Up to (excluding) 1.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	6.1	The Classima WordPress theme before 2.1.11 and some of its required plugins (Classified Listing before 2.2.14, Classified Listing Pro before 2.0.20, Classified Listing Store & Membership before 1.4.20 and Classima Core before 1.10) do not escape a parameter before outputting it back in attributes, leading to	N/A	A-RAD-CLAS-101022/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Reflected Cross-Site Scripting **CVE ID : CVE-2022-2654**		
Vendor: read_more_by_adam_project					
Product: read_more_by_adam					
Affected Version(s): * Up to (including) 1.1.8					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Read more By Adam plugin <= 1.1.8 at WordPress. **CVE ID : CVE-2022-38085**	https://patchstack.com/database/vulnerability/read-more/wordpress-read-more-by-adam-plugin-1-1-8-cross-site-request-forgery-csrf-vulnerability/_s_id=cve, https://wordpress.org/plugins/read-more/	A-REA-READ-101022/1084
Vendor: redis					
Product: redis					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.5					
Integer Overflow or Wraparound	23-Sep-2022	9.8	Redis is an in-memory database that persists on disk. Versions 7.0.0 and above, prior to 7.0.5 are vulnerable to an Integer Overflow. Executing an `XAUTOCLAIM` command on a stream key in a specific state, with a specially crafted `COUNT` argument	https://github.com/redis/redis/security/advisories/GHSA-5gc4-76rx-22c9	A-RED-REDI-101022/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause an integer overflow, a subsequent heap overflow, and potentially lead to remote code execution. This has been patched in Redis version 7.0.5. No known workarounds exist. **CVE ID : CVE-2022-35951**		
Vendor: rocket.chat					
Product: rocket.chat					
Affected Version(s): * Up to (excluding) 3.18.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	8.8	A SQL injection vulnerability exists in Rocket.Chat <v3.18.6, <v4.4.4 and <v4.7.3 which can allow an attacker to retrieve a reset password token through or a 2fa secret. **CVE ID : CVE-2022-32211**	N/A	A-ROC-ROCK-101022/1086
Affected Version(s): * Up to (excluding) 4.14.1.22788					
Improper Authentication	23-Sep-2022	6.8	An improper authentication vulnerability exists in Rocket.Chat Mobile App <4.14.1.22788 that allowed an attacker with physical access to a mobile device to bypass local	N/A	A-ROC-ROCK-101022/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication (PIN code). **CVE ID : CVE-2022-30124**		
Affected Version(s): * Up to (excluding) 4.6.4					
Insertion of Sensitive Information into Log File	23-Sep-2022	5.3	A cleartext storage of sensitive information exists in Rocket.Chat <v4.6.4 due to Oauth token being leaked in plaintext in Rocket.chat logs. **CVE ID : CVE-2022-32217**	N/A	A-ROC-ROCK-101022/1088
Affected Version(s): * Up to (excluding) 4.7.5					
Improper Authentication	23-Sep-2022	8.8	A improper authentication vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 that allowed two factor authentication can be bypassed when telling the server to use CAS during login. **CVE ID : CVE-2022-35248**	N/A	A-ROC-ROCK-101022/1089
Incorrect Permission Assignment for Critical Resource	23-Sep-2022	6.5	A cleartext transmission of sensitive information exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 relating to Oauth tokens by having the permission "view-full-other-user-info", this	N/A	A-ROC-ROCK-101022/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could cause an oauth token leak in the product. **CVE ID : CVE-2022-32227**		
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-2022	4.3	An information disclosure vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 due to the actionLinkHandler method was found to allow Message ID Enumeration with Regex MongoDB queries. **CVE ID : CVE-2022-32218**	N/A	A-ROC-ROCK-101022/1091
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-2022	4.3	An information disclosure vulnerability exists in Rocket.Chat <v4.7.5 which allowed the "users.list" REST endpoint gets a query parameter from JSON and runs Users.find(queryFromClientSide). This means virtually any authenticated user can access any data (except password hashes) of any user authenticated. **CVE ID : CVE-2022-32219**	N/A	A-ROC-ROCK-101022/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Sep-2022	4.3	An improper access control vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 due to input data in the getUsersOfRoom Meteor server method is not type validated, so that MongoDB query operator objects are accepted by the server, so that instead of a matching rid String a$regex query can be executed, bypassing the room access permission check for every but the first matching room. **CVE ID : CVE-2022-32226**	N/A	A-ROC-ROCK-101022/1093
Improper Input Validation	23-Sep-2022	4.3	An information disclosure vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 since the getReadReceipts Meteor server method does not properly filter user inputs that are passed to MongoDB queries, allowing $regex queries to enumerate	N/A	A-ROC-ROCK-101022/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary Message IDs. **CVE ID : CVE-2022-32228**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Sep-2022	4.3	A NoSQL-Injection information disclosure vulnerability vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 in the getS3FileUrl Meteor server method that can disclose arbitrary file upload URLs to users that should not be able to access. **CVE ID : CVE-2022-35246**	N/A	A-ROC-ROCK-101022/1095
Missing Authorization	23-Sep-2022	4.3	A information disclosure vulnerability exists in Rocket.chat <v5, <v4.8.2 and <v4.7.5 where the lack of ACL checks in the getRoomRoles Meteor method leak channel members with special roles to unauthorized clients. **CVE ID : CVE-2022-35247**	N/A	A-ROC-ROCK-101022/1096
Affected Version(s): * Up to (excluding) 5.0					
Exposure of Sensitive Information to an	23-Sep-2022	6.5	An information disclosure vulnerability exists in Rocket.Chat <v5	N/A	A-ROC-ROCK-101022/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			due to the getUserMentionsByChannel meteor server method discloses messages from private channels and direct messages regardless of the users access permission to the room. **CVE ID : CVE-2022-32220**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	A cross-site scripting vulnerability exists in Rocket.chat <v5 due to style injection in the complete chat window, an adversary is able to manipulate not only the style of it, but will also be able to block functionality as well as hijacking the content of targeted users. Hence the payloads are stored in messages, it is a persistent attack vector, which will trigger as soon as the message gets viewed. **CVE ID : CVE-2022-35251**	N/A	A-ROC-ROCK-101022/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Sep-2022	4.3	A information disclosure vulnerability exists in Rockert.Chat <v5 due to /api/v1/chat.getThreadsList lack of sanitization of user inputs and can therefore leak private thread messages to unauthorized users via Mongo DB injection. **CVE ID : CVE-2022-32229**	N/A	A-ROC-ROCK-101022/1099
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-2022	4.3	A information disclosure vulnerability exists in Rocket.Chat <v5 where the getUserMentionsByChannel meteor server method discloses messages from private channels and direct messages regardless of the users access permission to the room. **CVE ID : CVE-2022-35249**	N/A	A-ROC-ROCK-101022/1100
Incorrect Permission Assignment for Critical Resource	23-Sep-2022	4.3	A privilege escalation vulnerability exists in Rocket.chat <v5 which made it possible to elevate privileges for any authenticated user	N/A	A-ROC-ROCK-101022/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to view Direct messages without appropriate permissions. **CVE ID : CVE-2022-35250**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.4.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	8.8	A SQL injection vulnerability exists in Rocket.Chat <v3.18.6, <v4.4.4 and <v4.7.3 which can allow an attacker to retrieve a reset password token through or a 2fa secret. **CVE ID : CVE-2022-32211**	N/A	A-ROC-ROCK-101022/1102
Affected Version(s): From (including) 4.7.0 Up to (excluding) 4.7.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Sep-2022	8.8	A SQL injection vulnerability exists in Rocket.Chat <v3.18.6, <v4.4.4 and <v4.7.3 which can allow an attacker to retrieve a reset password token through or a 2fa secret. **CVE ID : CVE-2022-32211**	N/A	A-ROC-ROCK-101022/1103
Affected Version(s): From (including) 4.8.0 Up to (excluding) 4.8.2					
Improper Authentication	23-Sep-2022	8.8	A improper authentication vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 that allowed two factor authentication can	N/A	A-ROC-ROCK-101022/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be bypassed when telling the server to use CAS during login. **CVE ID : CVE-2022-35248**		
Incorrect Permission Assignment for Critical Resource	23-Sep-2022	6.5	A cleartext transmission of sensitive information exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 relating to Oauth tokens by having the permission "view-full-other-user-info", this could cause an oauth token leak in the product. **CVE ID : CVE-2022-32227**	N/A	A-ROC-ROCK-101022/1105
Exposure of Sensitive Information to an Unauthorized Actor	23-Sep-2022	4.3	An information disclosure vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 due to the actionLinkHandler method was found to allow Message ID Enumeration with Regex MongoDB queries. **CVE ID : CVE-2022-32218**	N/A	A-ROC-ROCK-101022/1106
Improper Input Validation	23-Sep-2022	4.3	An improper access control vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 due to input data in	N/A	A-ROC-ROCK-101022/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the getUsersOfRoom Meteor server method is not type validated, so that MongoDB query operator objects are accepted by the server, so that instead of a matching rid String a$regex query can be executed, bypassing the room access permission check for every but the first matching room. **CVE ID : CVE-2022-32226**		
Improper Input Validation	23-Sep-2022	4.3	An information disclosure vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 since the getReadReceipts Meteor server method does not properly filter user inputs that are passed to MongoDB queries, allowing $regex queries to enumerate arbitrary Message IDs. **CVE ID : CVE-2022-32228**	N/A	A-ROC-ROCK-101022/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Sep-2022	4.3	A NoSQL-Injection information disclosure vulnerability vulnerability exists in Rocket.Chat <v5, <v4.8.2 and <v4.7.5 in the getS3FileUrl Meteor server method that can disclose arbitrary file upload URLs to users that should not be able to access. **CVE ID : CVE-2022-35246**	N/A	A-ROC-ROCK-101022/1109
Missing Authorization	23-Sep-2022	4.3	A information disclosure vulnerability exists in Rocket.chat <v5, <v4.8.2 and <v4.7.5 where the lack of ACL checks in the getRoomRoles Meteor method leak channel members with special roles to unauthorized clients. **CVE ID : CVE-2022-35247**	N/A	A-ROC-ROCK-101022/1110
Vendor: Rockwellautomation					
Product: thinmanager					
Affected Version(s): From (including) 11.0.0 Up to (including) 13.0.0					
Out-of-bounds Write	23-Sep-2022	9.8	Rockwell Automation ThinManager ThinServer versions 11.0.0 - 13.0.0 is vulnerable	https://rockwellautomation.custhelp.com/app/answers/answe	A-ROC-THIN-101022/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a heap-based buffer overflow. An attacker could send a specifically crafted TFTP or HTTPS request, causing a heap-based buffer overflow that crashes the ThinServer process. If successfully exploited, this could expose the server to arbitrary remote code execution. **CVE ID : CVE-2022-38742**	r_view/a_id/1136847	
Vendor: ruby-arr-pm_project					
Product: ruby-arr-pm					
Affected Version(s): * Up to (excluding) 0.0.12					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Sep-2022	7.8	Arr-pm is an RPM reader/writer library written in Ruby. Versions prior to 0.0.12 are subject to OS command injection resulting in shell execution if the RPM contains a malicious "payload compressor" field. This vulnerability impacts the `extract` and `files` methods of the `RPM::File` class of this library. Version 0.0.12	https://github.com/jordansissel/ruby-arr-pm/pull/15, https://github.com/jordansissel/ruby-arr-pm/security/advisories/GHSA-88cv-mj24-8w3q, https://github.com/jordansissel/ruby-arr-pm/pull/14	A-RUB-RUBY-101022/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patches these issues. A workaround for this issue is to ensure any RPMs being processed contain valid/known payload compressor values such as gzip, bzip2, xz, zstd, and lzma. The payload compressor field in an rpm can be checked by using the rpm command line tool. **CVE ID : CVE-2022-39224**		
Vendor: safe					
Product: fme_server					
Affected Version(s): * Up to (excluding) 2021.2.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Sep-2022	7.2	Safe Software FME Server v2021.2.5, v2022.0.0.2 and below was discovered to contain a Path Traversal vulnerability via the component fmedataupload. **CVE ID : CVE-2022-38340**	https://community.safe.com/s/article/Known-Issue-FME-Server-vulnerability-with-arbitrary-path-traversal-and-file-upload	A-SAF-FME_-101022/1113
Improper Neutralization of Input During Web Page Generation	19-Sep-2022	6.1	Safe Software FME Server v2021.2.5, v2022.0.0.2 and below contains a cross-site scripting (XSS) vulnerability which allows	https://community.safe.com/s/article/FME-Server-Stored-Cross-Site-	A-SAF-FME_-101022/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the login page. **CVE ID : CVE-2022-38339**	Scripting-XSS-Vulnerabilities	
Affected Version(s): From (including) 2021.2.3 Up to (excluding) 2021.2.6					
Improper Input Validation	19-Sep-2022	7.1	Safe Software FME Server v2021.2.5 and below does not employ server-side validation. **CVE ID : CVE-2022-38341**	https://community.safe.com/s/article/Known-Issue-Lack-of-server-side-validation-when-creating-a-new-user-in-FME-Server	A-SAF-FME_-101022/1115
Affected Version(s): From (including) 2022.0.0.0 Up to (excluding) 2022.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Sep-2022	7.2	Safe Software FME Server v2021.2.5, v2022.0.0.2 and below was discovered to contain a Path Traversal vulnerability via the component fmedataupload. **CVE ID : CVE-2022-38340**	https://community.safe.com/s/article/Known-Issue-FME-Server-vulnerability-with-arbitrary-path-traversal-and-file-upload	A-SAF-FME_-101022/1116
Affected Version(s): From (including) 2022.0.0.0 Up to (excluding) 2022.0.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	6.1	Safe Software FME Server v2021.2.5, v2022.0.0.2 and below contains a cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary	https://community.safe.com/s/article/FME-Server-Stored-Cross-Site-Scripting-XSS-Vulnerabilities	A-SAF-FME_-101022/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web scripts or HTML via a crafted payload injected into the login page. **CVE ID : CVE-2022-38339**		
Vendor: Samsung					
Product: mtower					
Affected Version(s): * Up to (including) 0.3.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Sep-2022	7.5	A Buffer Access with Incorrect Length Value vulnerablity in the TEE_MACCompute Final function in Samsung mTower through 0.3.0 allows a trusted application to trigger a Denial of Service (DoS) by invoking the function TEE_MACCompute Final with an excessive size value of messageLen. **CVE ID : CVE-2022-40757**	https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/lib/libutee/tee_api_operations.c#L1031	A-SAM-MTOW-101022/1118
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Sep-2022	7.5	A Buffer Access with Incorrect Length Value vulnerablity in the TEE_CipherUpdate function in Samsung mTower through 0.3.0 allows a trusted application to trigger a Denial of Service (DoS) by	https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/lib/libutee/tee_api_operations.c#L1224	A-SAM-MTOW-101022/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invoking the function TEE_CipherUpdate with an excessive size value of srcLen. **CVE ID : CVE-2022-40758**		
NULL Pointer Dereference	16-Sep-2022	7.5	A NULL pointer dereference issue in the TEE_MACCompareFinal function in Samsung mTower through 0.3.0 allows a trusted application to trigger a Denial of Service (DoS) by invoking the function TEE_MACCompareFinal with a NULL pointer for the parameter operation. **CVE ID : CVE-2022-40759**	https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/lib/libutee/tee_api_operations.c#L1249	A-SAM-MTOW-101022/1120
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Sep-2022	7.5	A Buffer Access with Incorrect Length Value vulnerablity in the TEE_MACUpdate function in Samsung mTower through 0.3.0 allows a trusted application to trigger a Denial of Service (DoS) by invoking the function TEE_MACUpdate	https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/lib/libutee/tee_api_operations.c#L1188, https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5	A-SAM-MTOW-101022/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with an excessive size value of chunkSize. **CVE ID : CVE-2022-40760**	/crypto/libtomcrypt/include/tomcrypt_hash.h#L397	
Improper Input Validation	16-Sep-2022	7.5	The function tee_obj_free in Samsung mTower through 0.3.0 allows a trusted application to trigger a Denial of Service (DoS) by invoking the function TEE_AllocateOperation with a disturbed heap layout, related to utee_cryp_obj_alloc . **CVE ID : CVE-2022-40761**	https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/tee/tee_svc_cryp.c#L1248, https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/tee/tee_obj.c#L109	A-SAM-MTOW-101022/1122
Allocation of Resources Without Limits or Throttling	16-Sep-2022	7.5	A Memory Allocation with Excessive Size Value vulnerablity in the TEE_Realloc function in Samsung mTower through 0.3.0 allows a trusted application to trigger a Denial of Service (DoS) by invoking the function TEE_Realloc with an excessive number for the parameter len.	https://github.com/Samsung/mTower/blob/efd36709306a9afcca5b4782499d01be0c7a02a5/tee/lib/libutee/tee_api.c#L319	A-SAM-MTOW-101022/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40762		
Vendor: scala-lang					
Product: scala					
Affected Version(s): From (including) 2.13.0 Up to (excluding) 2.13.9					
Deserialization of Untrusted Data	23-Sep-2022	9.8	Scala 2.13.x before 2.13.9 has a Java deserialization chain in its JAR file. On its own, it cannot be exploited. There is only a risk in conjunction with LazyList object deserialization within an application. In such situations, it allows attackers to erase contents of arbitrary files, make network connections, or possibly run arbitrary code (specifically, Function0 functions) via a gadget chain. **CVE ID : CVE-2022-36944**	https://www.scala-lang.org/download/, https://github.com/scala/scala/pull/10118	A-SCA-SCAL-101022/1124
Vendor: school_activity_updates_with_sms_notification_project					
Product: school_activity_updates_with_sms_notification					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	16-Sep-2022	7.2	School Activity Updates with SMS Notification v1.0 is vulnerable to SQL Injection via /activity/admin/m	N/A	A-SCH-SCHO-101022/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			odules/department/index.php?view=edit&id=. **CVE ID : CVE-2022-38832**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	7.2	School Activity Updates with SMS Notification v1.0 is vulnerable to SQL Injection via /activity/admin/modules/modstudent/index.php?view=view&id=. **CVE ID : CVE-2022-38833**	N/A	A-SCH-SCHO-101022/1126
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	7.2	School Activity Updates with SMS Notification v1.0 is vulnerable to SQL Injection via /activity/admin/modules/event/index.php?view=edit&id=. **CVE ID : CVE-2022-38878**	N/A	A-SCH-SCHO-101022/1127
Vendor: scroll_to_top_project					
Product: scroll_to_top					
Affected Version(s): * Up to (excluding) 1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	4.8	The Scroll To Top WordPress plugin before 1.4.1 does not escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when	https://wpscan.com/vulnerability/f730f584-2370-49f9-a094-a5bc521671c1	A-SCR-SCRO-101022/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2710**		
Vendor: secp256k1-js_project					
Product: secp256k1-js					
Affected Version(s): * Up to (excluding) 1.1.0					
Improper Verification of Cryptographic Signature	24-Sep-2022	7.5	The secp256k1-js package before 1.1.0 for Node.js implements ECDSA without required r and s validation, leading to signature forgery. **CVE ID : CVE-2022-41340**	https://github.com/lionello/secp256k1-js/compare/1.0.1...1.1.0, https://github.com/lionello/secp256k1-js/commit/302800f0370b42e360a33774bb808274ac729c2e	A-SEC-SECP-101022/1129
Vendor: sedlex					
Product: favicon-switcher					
Affected Version(s): * Up to (including) 1.2.11					
Cross-Site Request Forgery (CSRF)	21-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in SedLex FavIcon Switcher plugin <= 1.2.11 at WordPress allows plugin settings change. **CVE ID : CVE-2022-40219**	https://wordpress.org/plugins/favicon-switcher/, https://patchstack.com/database/vulnerability/favicon-switcher/wordpress-favicon-switcher-plugin-1-2-11-cross-site-request-forgery-csrf-vulnerability	A-SED-FAVI-101022/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: seo_smart_links_project					
Product: seo_smart_links					
Affected Version(s): * Up to (including) 3.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	4.8	The SEO Smart Links WordPress plugin through 3.0.1 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 the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-3135**	N/A	A-SEO-SEO_-101022/1131
Vendor: sftpgo_project					
Product: sftpgo					
Affected Version(s): * Up to (excluding) 2.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	6.1	SFTPGo is an SFTP server written in Go. Versions prior to 2.3.5 are subject to Cross-site scripting (XSS) vulnerabilities in the SFTPGo WebClient, allowing remote attackers to inject malicious code. This issue is patched in version	https://github.com/drakkan/sftpgo/security/advisories/GHSA-cf7g-cm7q-rq7f	A-SFT-SFTP-101022/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.3.5. No known workarounds exist. **CVE ID : CVE-2022-39220**		
Vendor: simplefilelist					
Product: simple-file-list					
Affected Version(s): * Up to (excluding) 4.4.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	6.1	The Simple File List WordPress plugin before 4.4.12 does not escape parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-3062**	https://wpscan.com/vulnerability/2e829bbe-1843-496d-a852-4150fa6d1f7a	A-SIM-SIMP-101022/1133
Vendor: simple_bitcoin_faucets_project					
Product: simple_bitcoin_faucets					
Affected Version(s): * Up to (including) 1.7.0					
Cross-Site Request Forgery (CSRF)	26-Sep-2022	5.4	The Simple Bitcoin Faucets WordPress plugin through 1.7.0 does not have any authorisation and CSRF in an AJAX action, allowing any authenticated users, such as subscribers to call it and add/delete/edit Bonds. Furthermore, due to the lack of sanitisation and escaping, it could also lead to Stored	N/A	A-SIM-SIMP-101022/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting issues **CVE ID : CVE-2022-3024**		
Vendor: simple_college_website_project					
Product: simple_college_website					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	22-Sep-2022	9.8	Simple College Website v1.0 was discovered to contain an arbitrary file write vulnerability via the function file_put_contents(). This vulnerability allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2022-40087**	N/A	A-SIM-SIMP-101022/1135
N/A	22-Sep-2022	9.8	A remote file inclusion (RFI) vulnerability in Simple College Website v1.0 allows attackers to execute arbitrary code via a crafted PHP file. This vulnerability is exploitable when the directive allow_url_include is set to On. **CVE ID : CVE-2022-40089**	N/A	A-SIM-SIMP-101022/1136
Improper Neutralization of	22-Sep-2022	6.1	Simple College Website v1.0 was discovered to	N/A	A-SIM-SIMP-101022/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			contain a reflected cross-site scripting (XSS) vulnerability via the component /college_website/index.php?page=. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the page parameter. **CVE ID : CVE-2022-40088**		
Vendor: simple_task_managing_system_project					
Product: simple_task_managing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Sep-2022	9.8	SourceCodester Simple Task Managing System v1.0 was discovered to contain a SQL injection vulnerability via the bookId parameter at changeStatus.php. **CVE ID : CVE-2022-40030**	N/A	A-SIM-SIMP-101022/1138
Improper Neutralization of Special Elements used in an SQL Command	21-Sep-2022	7.2	SourceCodester Simple Task Managing System v1.0 was discovered to contain a SQL injection vulnerability via the bookId	N/A	A-SIM-SIMP-101022/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			parameter at board.php. **CVE ID : CVE-2022-40026**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	6.1	SourceCodester Simple Task Managing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component newTask.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the shortName parameter. **CVE ID : CVE-2022-40027**	N/A	A-SIM-SIMP-101022/1140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	4.8	SourceCodester Simple Task Managing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component newProjectValidation.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected	N/A	A-SIM-SIMP-101022/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into the fullName parameter. **CVE ID : CVE-2022-40028**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	4.8	SourceCodester Simple Task Managing System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component newProjectValidation.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the shortName parameter. **CVE ID : CVE-2022-40029**	N/A	A-SIM-SIMP-101022/1142
Vendor: snipeitapp					
Product: snipe-it					
Affected Version(s): * Up to (excluding) 6.0.10					
Improper Authentication	17-Sep-2022	4.3	Improper Authentication in GitHub repository snipe/snipe-it prior to 6.0.10. **CVE ID : CVE-2022-3173**	https://huntr.dev/bounties/6d8ffcc6-c6e3-4385-8ead-bdbbbacf79e9, https://github.com/snipe/snipe-it/commit/dcab1381e7ee0b7fd1df3a34750dbff4b79185b2	A-SNI-SNIP-101022/1143
Vendor: soflyy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_all_import					
Affected Version(s): * Up to (including) 3.6.7					
Unrestricted Upload of File with Dangerous Type	21-Sep-2022	7.2	Authenticated Arbitrary Code Execution vulnerability in Soflyy Import any XML or CSV File to WordPress plugin <= 3.6.7 at WordPress. **CVE ID : CVE-2022-36386**	https://wordpress.org/plugins/wp-all-import/#developers, https://patchstack.com/database/vulnerability/wp-all-import/wordpress-import-any-xml-or-csv-file-to-wordpress-plugin-3-6-7-authenticated-arbitrary-code-execution-vulnerability	A-SOF-WP_A-101022/1144
Vendor: Sophos					
Product: firewall					
Affected Version(s): * Up to (including) 19.0.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Sep-2022	9.8	A code injection vulnerability in the User Portal and Webadmin allows a remote attacker to execute code in Sophos Firewall version v19.0 MR1 and older. **CVE ID : CVE-2022-3236**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20220923-sfos-rce	A-SOP-FIRE-101022/1145
Vendor: stealjs					
Product: steal					
Affected Version(s): 2.2.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	16-Sep-2022	9.8	Prototype pollution vulnerability in function convertLater in npm-convert.js in stealjs steal 2.2.4 via the packageName variable in npm-convert.js. **CVE ID : CVE-2022-37258**	N/A	A-STE-STEA-101022/1146
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	20-Sep-2022	9.8	Prototype pollution vulnerability in stealjs steal 2.2.4 via the alias variable in babel.js. **CVE ID : CVE-2022-37265**	https://github.com/stealjs/steal/blob/c9dd1eb19ed3f97aeb93cf9dcea5d68ad5d0ced9/ext/babel.js#L4569, https://github.com/stealjs/steal/blob/c9dd1eb19ed3f97aeb93cf9dcea5d68ad5d0ced9/ext/babel.js#L4216	A-STE-STEA-101022/1147
Uncontrolled Resource Consumption	20-Sep-2022	7.5	A Regular Expression Denial of Service (ReDoS) flaw was found in stealjs steal 2.2.4 via the string variable in babel.js. **CVE ID : CVE-2022-37259**	N/A	A-STE-STEA-101022/1148
Vendor: strapi					
Product: strapi					
Affected Version(s): * Up to (excluding) 3.6.10					
Improper Neutralization of	27-Sep-2022	8.8	Strapi before 3.6.10 and 4.x before 4.1.10	N/A	A-STR-STRA-101022/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			mishandles hidden attributes within admin API responses. **CVE ID : CVE-2022-31367**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.1.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Sep-2022	8.8	Strapi before 3.6.10 and 4.x before 4.1.10 mishandles hidden attributes within admin API responses. **CVE ID : CVE-2022-31367**	N/A	A-STR-STRA-101022/1150
Vendor: sucuri					
Product: security					
Affected Version(s): * Up to (including) 1.8.33					
Cross-Site Request Forgery (CSRF)	16-Sep-2022	4.3	Cross-Site Request Forgery (CSRF) vulnerability in Sucuri Security plugin <= 1.8.33 at WordPress leading to Event log entry creation. **CVE ID : CVE-2022-29489**	https://patchstack.com/database/vulnerability/sucuri-scanner/wordpress-sucuri-security-plugin-1-8-33-cross-site-request-forgery-csrf-vulnerability, https://wordpress.org/plugins/sucuri-scanner/#developers	A-SUC-SECU-101022/1151
Vendor: supremainc					
Product: biostar_2					
Affected Version(s): 2.8.16					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	19-Sep-2022	8.8	A vulnerability in Suprema BioStar (aka Bio Star) 2 v2.8.16 allows attackers to escalate privileges to System Administrator via a crafted PUT request to the update profile page. **CVE ID : CVE-2022-38351**	N/A	A-SUP-BIOS-101022/1152
Vendor: svg_support_wordpress					
Product: svg_support					
Affected Version(s): * Up to (excluding) 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	5.4	The SVG Support WordPress plugin before 2.5 does not properly handle SVG added via an URL, which could allow users with a role as low as author to perform Cross-Site Scripting attacks **CVE ID : CVE-2022-1755**	https://wpscan.com/vulnerability/62b2548e-6b59-48b8-b1c2-9bd47e634982	A-SVG-SVG_-101022/1153
Vendor: Swftools					
Product: swftools					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	21-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a memory leak via /lib/mem.c.	N/A	A-SWF-SWFT-101022/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35085		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via /multiarch/memmove-vec-unaligned-erms.S. **CVE ID : CVE-2022-35086**	N/A	A-SWF-SWFT-101022/1155
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via MovieAddFrame at /src/gif2swf.c. **CVE ID : CVE-2022-35087**	N/A	A-SWF-SWFT-101022/1156
Out-of-bounds Write	21-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap buffer-overflow via getGifDelayTime at /home/bupt/Desktop/swftools/src/src/gif2swf.c. **CVE ID : CVE-2022-35088**	N/A	A-SWF-SWFT-101022/1157
Allocation of Resources Without Limits or Throttling	21-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer-overflow via getTransparentColor at /home/bupt/Deskt	N/A	A-SWF-SWFT-101022/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			op/swftools/src/gif2swf. **CVE ID : CVE-2022-35089**		
Out-of-bounds Write	21-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via __asan_memcpy at /asan/asan_interceptors_memintrinsics.cpp:. **CVE ID : CVE-2022-35090**	N/A	A-SWF-SWFT-101022/1159
Affected Version(s): 2021-12-16					
Out-of-bounds Write	20-Sep-2022	9.8	SWFTools commit 772e55a was discovered to contain a heap-buffer overflow via the function readU8 at /lib/ttf.c. **CVE ID : CVE-2022-40008**	N/A	A-SWF-SWFT-101022/1160
Use After Free	20-Sep-2022	9.8	SWFTools commit 772e55a was discovered to contain a heap-use-after-free via the function grow_unicode at /lib/ttf.c. **CVE ID : CVE-2022-40009**	N/A	A-SWF-SWFT-101022/1161
Incorrect Comparison	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a floating point exception (FPE) via	N/A	A-SWF-SWFT-101022/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DCTStream::readMCURow() at /xpdf/Stream.cc.ow() **CVE ID : CVE-2022-35091**		
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via convert_gfxline at /gfxpoly/convert.c. **CVE ID : CVE-2022-35092**	N/A	A-SWF-SWFT-101022/1163
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a global buffer overflow via DCTStream::transformDataUnit at /xpdf/Stream.cc. **CVE ID : CVE-2022-35093**	N/A	A-SWF-SWFT-101022/1164
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via DCTStream::readHuffSym(DCTHuffTable*) at /xpdf/Stream.cc. **CVE ID : CVE-2022-35094**	N/A	A-SWF-SWFT-101022/1165
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a	N/A	A-SWF-SWFT-101022/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			segmentation violation via InfoOutputDev::type3D1 at /pdf/InfoOutputDev.cc. **CVE ID : CVE-2022-35095**		
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via draw_stroke at /gfxpoly/stroke.c. **CVE ID : CVE-2022-35096**	N/A	A-SWF-SWFT-101022/1167
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via FoFiTrueType::writeTTF at /xpdf/FoFiTrueType.cc. **CVE ID : CVE-2022-35097**	N/A	A-SWF-SWFT-101022/1168
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via GfxICCBasedColorSpace::getDefaultColor(GfxColor*) at /xpdf/GfxState.cc. **CVE ID : CVE-2022-35098**	N/A	A-SWF-SWFT-101022/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	5.5	SWFTools commit 772e55a2 was discovered to contain a stack overflow via ImageStream::getPixel(unsigned char*) at /xpdf/Stream.cc. **CVE ID : CVE-2022-35099**	N/A	A-SWF-SWFT-101022/1170
Vendor: symfony					
Product: twig					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.44.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	7.5	Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/../some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of	https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b, https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33, https://www.drupal.org/sa-core-2022-016	A-SYM-TWIG-101022/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such template names. There are no known workarounds aside from upgrading. **CVE ID : CVE-2022-39261**		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.15.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	7.5	Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/../some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading.	https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b, https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33, https://www.drupal.org/sa-core-2022-016	A-SYM-TWIG-101022/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39261		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.4.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	7.5	Twig is a template language for PHP. Versions 1.x prior to 1.44.7, 2.x prior to 2.15.3, and 3.x prior to 3.4.3 encounter an issue when the filesystem loader loads templates for which the name is a user input. It is possible to use the `source` or `include` statement to read arbitrary files from outside the templates' directory when using a namespace like `@somewhere/../some.file`. In such a case, validation is bypassed. Versions 1.44.7, 2.15.3, and 3.4.3 contain a fix for validation of such template names. There are no known workarounds aside from upgrading. **CVE ID : CVE-2022-39261**	https://github.com/twigphp/Twig/commit/35f3035c5deb0041da7b84daf02dea074ddc7a0b, https://github.com/twigphp/Twig/security/advisories/GHSA-52m2-vc4m-jj33, https://www.drupal.org/sa-core-2022-016	A-SYM-TWIG-101022/1173
Vendor: syncovery					
Product: syncovery					
Affected Version(s): From (including) 8.00 Up to (excluding) 9.48j					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	16-Sep-2022	9.8	An issue in the component post_applogin.php of Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below allows attackers to escalate privileges via creating crafted session tokens. **CVE ID : CVE-2022-36536**	N/A	A-SYN-SYNC-101022/1174
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Sep-2022	8.8	Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below was discovered to contain multiple remote code execution (RCE) vulnerabilities via the Job_ExecuteBefore and Job_ExecuteAfter parameters at post_profilesettings.php. **CVE ID : CVE-2022-36534**	N/A	A-SYN-SYNC-101022/1175
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below was discovered to contain a cross-site scripting (XSS) vulnerability.	N/A	A-SYN-SYNC-101022/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36533		
Vendor: tabs_project					
Product: tabs					
Affected Version(s): * Up to (including) 3.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities in Tabs plugin <= 3.7.1 at WordPress. **CVE ID : CVE-2022-40215**	https://patchstack.com/database/vulnerability/vc-tabs/wordpress-tabs-plugin-3-7-1-multiple-authenticated-stored-cross-site-scripting-xss-vulnerabilities/_s_id=cve, https://wordpress.org/plugins/vc-tabs/	A-TAB-TABS-101022/1177
Vendor: Tesla					
Product: tesla					
Affected Version(s): 4.23					
Authentication Bypass by Spoofing	16-Sep-2022	5.3	Tesla Model 3 V11.0(2022.4.5.16b701552d7a6) Tesla mobile app v4.23 is vulnerable to Authentication Bypass by spoofing. Tesla Model 3's Phone Key authentication is vulnerable to Man-in-the-middle attacks in the BLE channel. It allows attackers to open a door and drive the car away by	N/A	A-TES-TESL-101022/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leveraging access to a legitimate Phone Key. **CVE ID : CVE-2022-37709**		
Vendor: Testlink					
Product: testlink					
Affected Version(s): 1.9.20					
Cross-Site Request Forgery (CSRF)	20-Sep-2022	8.8	TestLink v1.9.20 was discovered to contain a Cross-Site Request Forgery (CSRF) via /lib/plan/planView.php. **CVE ID : CVE-2022-35196**	N/A	A-TES-TEST-101022/1179
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	7.2	TestLink v1.9.20 was discovered to contain a SQL injection vulnerability via /lib/execute/execNavigator.php. **CVE ID : CVE-2022-35193**	N/A	A-TES-TEST-101022/1180
N/A	16-Sep-2022	7.2	TestLink 1.9.20 Raijin was discovered to contain a broken access control vulnerability at /lib/attachments/attachmentdownload.php **CVE ID : CVE-2022-35195**	N/A	A-TES-TEST-101022/1181
Improper Neutralization of	16-Sep-2022	5.4	TestLink v1.9.20 was discovered to contain a stored	N/A	A-TES-TEST-101022/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			cross-site scripting (XSS) vulnerability via /lib/inventory/inventoryView.php. **CVE ID : CVE-2022-35194**		
Vendor: themehunk					
Product: wp_popup_builder					
Affected Version(s): * Up to (including) 1.2.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	6.1	The WP Popup Builder WordPress plugin through 1.2.8 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-2404**	https://wpscan.com/vulnerability/0d889dde-b9d5-46cf-87d3-4f8a85cf9b98	A-THE-WP_P-101022/1183
Cross-Site Request Forgery (CSRF)	26-Sep-2022	4.3	The WP Popup Builder WordPress plugin through 1.2.8 does not have authorisation and CSRF check in an AJAX action, allowing any authenticated users, such as subscribers to delete arbitrary Popup **CVE ID : CVE-2022-2405**	N/A	A-THE-WP_P-101022/1184
Vendor: themesawesome					
Product: timeline_awesome					
Affected Version(s): * Up to (including) 1.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Authenticated (author+) Stored Cross-Site Scripting (XSS) vulnerability in Themes Awesome History Timeline plugin <= 1.0.5 at WordPress. **CVE ID : CVE-2022-37328**	https://patchstack.com/database/vulnerability/timeline-awesome/wordpress-history-timeline-plugin-1-0-5-authenticated-stored-cross-site-scripting-xss-vulnerability/_s_id=cve, https://wordpress.org/plugins/timeline-awesome/	A-THE-TIME-101022/1185
Vendor: Tibco					
Product: ebx					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	9	The Web Server component of TIBCO Software Inc.'s TIBCO EBX contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker.	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/09/tibco-security-advisory-september-21-2022-tibco-ebx-cve-2022-30577	A-TIB-EBX-101022/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions 6.0.0 through 6.0.8. **CVE ID : CVE-2022-30577**		
Product: ebx_add-ons					
Affected Version(s): * Up to (excluding) 5.4.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	9	The Web Server component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 5.4.1 and below. **CVE ID : CVE-2022-30578**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/09/tibco-security-advisory-september-21-2022-tibco-ebx-add-ons-cve-2022	A-TIB-EBX_-101022/1187
Product: spotfire_analytics_platform					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 12.0.0					
Server-Side Request Forgery (SSRF)	20-Sep-2022	8.4	The Web Player component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a difficult to exploit vulnerability that allows a low privileged attacker with network access to execute blind Server Side Request Forgery (SSRF) on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 12.0.0 and TIBCO Spotfire Server: version 12.0.0. **CVE ID : CVE-2022-30579**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/09/tibco-security-advisory-september-20-2022-tibco-spotfire-cve-2022-30579	A-TIB-SPOT-101022/1188
Product: spotfire_server					
Affected Version(s): 12.0.0					
Server-Side Request Forgery (SSRF)	20-Sep-2022	8.4	The Web Player component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2	A-TIB-SPOT-101022/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TIBCO Spotfire Server contains a difficult to exploit vulnerability that allows a low privileged attacker with network access to execute blind Server Side Request Forgery (SSRF) on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 12.0.0 and TIBCO Spotfire Server: version 12.0.0. **CVE ID : CVE-2022-30579**	022/09/tibco-security-advisory-september-20-2022-tibco-spotfire-cve-2022-30579	
Vendor: tinyproxy_project					
Product: tinyproxy					
Affected Version(s): * Up to (excluding) 2022-09-08					
Insecure Default Initialization of Resource	19-Sep-2022	7.5	Tinyproxy commit 84f203f and earlier does not process HTTP request lines in the process_request() function and is using uninitialized buffers. This vulnerability allows attackers to access sensitive information at system runtime.	N/A	A-TIN-TINY-101022/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40468		
Vendor: tooljet					
Product: tooljet					
Affected Version(s): * Up to (excluding) 2022-09-11					
Exposure of Sensitive Information to an Unauthorized Actor	28-Sep-2022	4.9	Just like in the previous report, an attacker could steal the account of different users. But in this case, it's a little bit more specific, because it is needed to be an editor in the same app as the victim. **CVE ID : CVE-2022-3348**	https://huntr.dev/bounties/aae4aeb8-2612-4254-85e5-90675b082eac, https://github.com/tooljet/tooljet/commit/37bf6de75f161e03c2a81888810488b913863a46	A-TOO-TOOL-101022/1191
Vendor: topdigitaltrends					
Product: mega_addons_for_wpbakery_page_builder					
Affected Version(s): * Up to (including) 4.2.7					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Topdigitaltrends Mega Addons For WPBakery Page Builder plugin <= 4.2.7 at WordPress. **CVE ID : CVE-2022-36798**	https://patchstack.com/database/vulnerability/mega-addons-for-visual-composer/wordpress-mega-addons-for-wpbakery-page-builder-plugin-4-2-7-cross-site-request-forgery-csrf-vulnerability, https://wordpress.org/plugins/mega-addons-for-visual-composer/	A-TOP-MEGA-101022/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: total-soft					
Product: event_calendar					
Affected Version(s): * Up to (including) 1.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Sep-2022	5.4	Authenticated (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Totalsoft Event Calendar – Calendar plugin <= 1.4.6 at WordPress. **CVE ID : CVE-2022-36390**	https://patchstack.com/database/vulnerability/calendar-event/wordpress-event-calendar-calendar-plugin-1-4-6-authenticated-reflected-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/calendar-event/#developers	A-TOT-EVEN-101022/1193
Vendor: Trendmicro					
Product: apex_one					
Affected Version(s): -					
Improper Authentication	19-Sep-2022	9.8	A vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service could allow an attacker to bypass the product's login authentication by falsifying request parameters on affected installations. **CVE ID : CVE-2022-40144**	https://www.ipa.go.jp/security/ciadr/vul/20220913-jvn.html, https://success.trendmicro.com/solution/000291528, https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=4553, https://jvn.jp/en/jp/JVN36454862/index.html	A-TRE-APEX-101022/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	19-Sep-2022	7.8	A security link following local privilege escalation vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service agents could allow a local attacker to create a writable folder in an arbitrary location and escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40142**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1195
Inadequate Encryption Strength	19-Sep-2022	7.5	A vulnerability in Trend Micro Apex One and Apex One as a Service could allow an attacker to intercept and decode certain communication strings that may contain some identification attributes of a particular Apex One server. **CVE ID : CVE-2022-40141**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	19-Sep-2022	7.3	A link following local privilege escalation vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service servers could allow a local attacker to abuse an insecure directory that could allow a low-privileged user to run arbitrary code with elevated privileges. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40143**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1197
Improper Input Validation	19-Sep-2022	7.2	Improper validation of some components used by the rollback mechanism in Trend Micro Apex One and Trend Micro Apex One as a Service clients could allow a Apex One server administrator to instruct affected clients to download an unverified rollback package,	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could lead to remote code execution. Please note: an attacker must first obtain Apex One server administration console access in order to exploit this vulnerability. **CVE ID : CVE-2022-40139**		
Origin Validation Error	19-Sep-2022	5.5	An origin validation error vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to cause a denial-of-service on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40140**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1199
Affected Version(s): 2019					
Improper Authentication	19-Sep-2022	9.8	A vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service could allow an attacker to bypass the product's login	https://www.ipa.go.jp/security/ciadr/vul/20220913-jvn.html, https://success.trendmicro.com/solution/000291528,	A-TRE-APEX-101022/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication by falsifying request parameters on affected installations. **CVE ID : CVE-2022-40144**	https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=4553, https://jvn.jp/en/jp/JVN36454862/index.html	
Improper Privilege Management	19-Sep-2022	7.8	A security link following local privilege escalation vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service agents could allow a local attacker to create a writable folder in an arbitrary location and escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40142**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1201
Inadequate Encryption Strength	19-Sep-2022	7.5	A vulnerability in Trend Micro Apex One and Apex One as a Service could allow an attacker to intercept and decode certain communication strings that may	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain some identification attributes of a particular Apex One server. **CVE ID : CVE-2022-40141**		
Improper Link Resolution Before File Access ('Link Following')	19-Sep-2022	7.3	A link following local privilege escalation vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service servers could allow a local attacker to abuse an insecure directory that could allow a low-privileged user to run arbitrary code with elevated privileges. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40143**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1203
Improper Input Validation	19-Sep-2022	7.2	Improper validation of some components used by the rollback mechanism in Trend Micro Apex One and Trend Micro Apex One as a Service clients	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow a Apex One server administrator to instruct affected clients to download an unverified rollback package, which could lead to remote code execution. Please note: an attacker must first obtain Apex One server administration console access in order to exploit this vulnerability. **CVE ID : CVE-2022-40139**		
Origin Validation Error	19-Sep-2022	5.5	An origin validation error vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to cause a denial-of-service on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40140**	https://success.trendmicro.com/solution/000291528	A-TRE-APEX-101022/1205
Product: deep_security					
Affected Version(s): 20.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	28-Sep-2022	7.8	A link following vulnerability in Trend Micro Deep Security 20 and Cloud One - Workload Security Agent for Windows could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40710**	https://success.trendmicro.com/solution/000291590	A-TRE-DEEP-101022/1206
Out-of-bounds Read	28-Sep-2022	3.3	An Out-of-bounds read vulnerability in Trend Micro Deep Security 20 and Cloud One - Workload Security Agent for Windows could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these	https://success.trendmicro.com/solution/000291590	A-TRE-DEEP-101022/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities. This vulnerability is similar to, but not identical to CVE-2022-40708. **CVE ID : CVE-2022-40707**		
Out-of-bounds Read	28-Sep-2022	3.3	An Out-of-bounds read vulnerability in Trend Micro Deep Security 20 and Cloud One - Workload Security Agent for Windows could allow a local attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these vulnerabilities. This vulnerability is similar to, but not identical to CVE-2022-40707. **CVE ID : CVE-2022-40708**	https://success.trendmicro.com/solution/000291590	A-TRE-DEEP-101022/1208
Out-of-bounds Read	28-Sep-2022	3.3	An Out-of-bounds read vulnerability in Trend Micro Deep Security 20 and Cloud One - Workload Security Agent for Windows could allow a local	https://success.trendmicro.com/solution/000291590	A-TRE-DEEP-101022/1209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose sensitive information on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit these vulnerabilities. This vulnerability is similar to, but not identical to CVE-2022-40707 and 40708. **CVE ID : CVE-2022-40709**		
Product: housecall					
Affected Version(s): * Up to (including) 1.62.1.1133					
Incorrect Default Permissions	19-Sep-2022	7.8	A vulnerability on Trend Micro HouseCall version 1.62.1.1133 and below could allow a local attacker to escalate privlieges due to an overly permissive folder om the product installer. **CVE ID : CVE-2022-38764**	https://helpcenter.trendmicro.com/en-us/article/tmka-11092	A-TRE-HOUS-101022/1210
Product: mobile_security					
Affected Version(s): 9.8					
N/A	19-Sep-2022	9.1	A potential unathenticated file deletion	https://files.trendmicro.com/documentation/r	A-TRE-MOBI-101022/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilty on Trend Micro Mobile Security for Enterprise 9.8 SP5 could allow an attacker with access to the Management Server to delete files. This issue was resolved in 9.8 SP5 Critical Patch 2. **CVE ID : CVE-2022-40980**	eadme/tmms_sp5_cp2/tmms-ee_9.8_sp5_patch2_readme_server.txt	
Product: security					
Affected Version(s): * Up to (including) 17.7.1179					
Improper Link Resolution Before File Access ('Link Following')	19-Sep-2022	7.8	Trend Micro Security 2022 (consumer) has a link following vulnerability where an attacker with lower privileges could manipulate a mountpoint which could lead to escalation of privilege on an affected machine. **CVE ID : CVE-2022-34893**	https://helpcenter.trendmicro.com/en-us/article/tmka-11053	A-TRE-SECU-101022/1212
Affected Version(s): * Up to (including) 17.7.1383					
Out-of-bounds Read	19-Sep-2022	5.5	Trend Micro Security 2021 and 2022 (Consumer) is vulnerable to an Out-Of-Bounds Read Information Disclosure Vulnerability that could allow an	https://helpcenter.trendmicro.com/en-us/article/tmka-11058	A-TRE-SECU-101022/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to read sensitive information from other memory locations and cause a crash on an affected machine. This vulnerability is similar to, but not the same as CVE-2022-35234. **CVE ID : CVE-2022-37347**		
Out-of-bounds Read	19-Sep-2022	5.5	Trend Micro Security 2021 and 2022 (Consumer) is vulnerable to an Out-Of-Bounds Read Information Disclosure Vulnerability that could allow an attacker to read sensitive information from other memory locations and cause a crash on an affected machine. This vulnerability is similar to, but not the same as CVE-2022-37347. **CVE ID : CVE-2022-37348**	https://helpcenter.trendmicro.com/en-us/article/tmka-11058	A-TRE-SECU-101022/1214
Vendor: trudesk_project					
Product: trudesk					
Affected Version(s): * Up to (excluding) 1.2.2					
Integer Overflow or	29-Sep-2022	7.5	The trudesk application allows large characters to insert in the input	https://huntr.dev/bounties/1ff8afe4-6ff7-45aa-a652-	A-TRU-TRUD-101022/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			field "Full Name" on the signup field which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request in GitHub repository polonel/trudesk prior to 1.2.2. This can lead to Denial of service. **CVE ID : CVE-2022-1718**	d8aac7e5be7e, https://github.com/polonel/trudesk/commit/87e231e04495fb705fe1e03cb56fc4136bafe895	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Sep-2022	5.4	Reflected XSS on ticket filter function in GitHub repository polonel/trudesk prior to 1.2.2. This vulnerability is capable of executing a malicious javascript code in web page **CVE ID : CVE-2022-1719**	https://huntr.dev/bounties/790ba3fd-41e9-4393-8e2f-71161b56279b, https://github.com/polonel/trudesk/commit/36a542abbbb74828338ce402d65653ac58db42e0	A-TRU-TRUD-101022/1216
Vendor: ucms_project					
Product: ucms					
Affected Version(s): 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	6.1	UCMS v1.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Import function under the Site Management page. **CVE ID : CVE-2022-38527**	N/A	A-UCM-UCMS-101022/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ui					
Product: desktop					
Affected Version(s): * Up to (excluding) 0.55.3.17					
N/A	23-Sep-2022	7.8	A local privilege escalation vulnerability in UI Desktop for Windows (Version 0.55.1.2 and earlier) allows a malicious actor with local access to a Windows device with UI Desktop to run arbitrary commands as SYSTEM. **CVE ID : CVE-2022-35257**	https://community.ui.com/releases/Security-Advisory-Bulletin-025-025/7fc92851-054d-46d3-bdb0-fbb8f7023fed	A-UI-DESK-101022/1218
Vendor: valine.js					
Product: valine					
Affected Version(s): 1.4.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	9.6	Valine v1.4.18 was discovered to contain a remote code execution (RCE) vulnerability which allows attackers to execute arbitrary code via a crafted POST request. **CVE ID : CVE-2022-38545**	N/A	A-VAL-VALI-101022/1219
Vendor: Veritas					
Product: desktop_and_laptop_option					
Affected Version(s): From (including) 9.1 Up to (excluding) 9.8					
Improper Neutralizat	23-Sep-2022	6.1	A Reflected Cross-Site Scripting (XSS)	https://www.veritas.com/conte	A-VER-DESK-101022/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerability affects the Veritas Desktop Laptop Option (DLO) application login page (aka the DLOServer/restore/login.jsp URI). This affects versions before 9.8 (e.g., 9.1 through 9.7). **CVE ID : CVE-2022-41319**	nt/support/en_US/security/VTS22-010	
Product: system_recovery					
Affected Version(s): From (including) 18.0 Up to (excluding) 18.0.4.57090					
Insecure Storage of Sensitive Information	23-Sep-2022	6.5	Veritas System Recovery (VSR) versions 18 and 21 store a network destination password in the Windows registry during configuration of the backup configuration. This vulnerability could provide a Windows user (who has sufficient privileges) to access a network file system that they were not authorized to access. **CVE ID : CVE-2022-41320**	https://www.veritas.com/content/support/en_US/security/VTS21-002	A-VER-SYST-101022/1221
Affected Version(s): From (including) 21 Up to (excluding) 21.0.3.62140					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insecure Storage of Sensitive Information	23-Sep-2022	6.5	Veritas System Recovery (VSR) versions 18 and 21 store a network destination password in the Windows registry during configuration of the backup configuration. This vulnerability could provide a Windows user (who has sufficient privileges) to access a network file system that they were not authorized to access. **CVE ID : CVE-2022-41320**	https://www.veritas.com/content/support/en_US/security/VTS21-002	A-VER-SYST-101022/1222
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 8.2.4959					
NULL Pointer Dereference	29-Sep-2022	5.5	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.4959. **CVE ID : CVE-2022-1725**	https://huntr.dev/bounties/4363cf07-233e-4d0a-a1d5-c731a400525c, https://github.com/vim/vim/commit/b62dc5e7825bc195efe3041d5b3a9f1528359e1c	A-VIM-VIM-101022/1223
Affected Version(s): * Up to (excluding) 9.0.0483					
Out-of-bounds Write	17-Sep-2022	7.8	Heap-based Buffer Overflow in GitHub repository	https://github.com/vim/vim/commit/c249913edc35c0e666d	A-VIM-VIM-101022/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vim/vim prior to 9.0.0483. **CVE ID : CVE-2022-3234**	783bfc21595cf9f7d9e0d, https://huntr.dev/bounties/90fdf374-bf04-4386-8a23-38c83b88f0da	
Affected Version(s): * Up to (excluding) 9.0.0490					
Use After Free	18-Sep-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0.0490. **CVE ID : CVE-2022-3235**	https://huntr.dev/bounties/96d5f7a0-a834-4571-b73b-0fe523b941af, https://github.com/vim/vim/commit/1c3dd8ddcba63c1af5112e567215b3cec2de11d0	A-VIM-VIM-101022/1225
Affected Version(s): * Up to (excluding) 9.0.0530					
Use After Free	22-Sep-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0.0530. **CVE ID : CVE-2022-3256**	https://github.com/vim/vim/commit/8ecfa2c56b4992c7f067b92488aa9acea5a454ad, https://huntr.dev/bounties/8336a3df-212a-4f8d-ae34-76ef1f936bb3	A-VIM-VIM-101022/1226
Affected Version(s): * Up to (excluding) 9.0.0552					
NULL Pointer Dereference	23-Sep-2022	5.5	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0552. **CVE ID : CVE-2022-3278**	https://github.com/vim/vim/commit/69082916c8b5d321545d60b9f5facad0a2dd5a4e, https://huntr.dev/bounties/a9fad77e-f245-	A-VIM-VIM-101022/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4ce9-ba15-c7d4c86c4612	
Affected Version(s): * Up to (excluding) 9.0.0577					
Stack-based Buffer Overflow	25-Sep-2022	7.8	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0577. **CVE ID : CVE-2022-3296**	https://github.com/vim/vim/commit/96b9bf8f74af8abf1e30054f996708db7dc285be, https://huntr.dev/bounties/958866b8-526a-4979-9471-39392e0c9077	A-VIM-VIM-101022/1228
Affected Version(s): * Up to (excluding) 9.0.0579					
Use After Free	25-Sep-2022	7.8	Use After Free in GitHub repository vim/vim prior to 9.0.0579. **CVE ID : CVE-2022-3297**	https://github.com/vim/vim/commit/0ff01835a40f549c5c4a550502f62a2ac9ac447c, https://huntr.dev/bounties/1aa9ec92-0355-4710-bf85-5bce9effa01c	A-VIM-VIM-101022/1229
Affected Version(s): * Up to (excluding) 9.0.0598					
Out-of-bounds Write	27-Sep-2022	7.8	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0598. **CVE ID : CVE-2022-3324**	https://huntr.dev/bounties/e414e55b-f332-491f-863b-c18dca97403c, https://github.com/vim/vim/commit/8279af514ca7e5fd3c31cf13b0864163d1a0bfeb	A-VIM-VIM-101022/1230
Affected Version(s): * Up to (excluding) 9.0.0614					
Use After Free	29-Sep-2022	7.8	Use After Free in GitHub repository	https://huntr.dev/bounties/d0	A-VIM-VIM-101022/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vim/vim prior to 9.0.0614. **CVE ID : CVE-2022-3352**	58f182-a49b-40c7-9234-43d4c5a29f60, https://github.com/vim/vim/commit/ef976323e770315b5fca544efb6b2faa25674d15	
Vendor: visam					
Product: vbase					
Affected Version(s): 11.7.0.2					
N/A	16-Sep-2022	7.5	When logging in to a VBASE runtime project via Web-Remote, the product uses XOR with a static initial key to obfuscate login messages. An unauthenticated remote attacker with the ability to capture a login session can obtain the login credentials. **CVE ID : CVE-2022-3217**	N/A	A-VIS-VBAS-101022/1232
Vendor: Vmware					
Product: spring_data_rest					
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.7					
N/A	21-Sep-2022	3.7	Applications that allow HTTP PATCH access to resources exposed by Spring Data REST in versions 3.6.0 - 3.5.5, 3.7.0 - 3.7.2, and older unsupported	https://tanzu.vmware.com/security/cve-2022-31679	A-VMW-SPRI-101022/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions, if an attacker knows about the structure of the underlying domain model, they can craft HTTP requests that expose hidden entity attributes. **CVE ID : CVE-2022-31679**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.3					
N/A	21-Sep-2022	3.7	Applications that allow HTTP PATCH access to resources exposed by Spring Data REST in versions 3.6.0 - 3.5.5, 3.7.0 - 3.7.2, and older unsupported versions, if an attacker knows about the structure of the underlying domain model, they can craft HTTP requests that expose hidden entity attributes. **CVE ID : CVE-2022-31679**	https://tanzu.vmware.com/security/cve-2022-31679	A-VMW-SPRI-101022/1234
Vendor: Vtiger					
Product: vtiger_crm					
Affected Version(s): * Up to (including) 7.4.0					
Improper Neutralization of Input During Web Page	27-Sep-2022	5.4	Vtiger CRM v7.4.0 was discovered to contain a stored cross-site scripting (XSS) vulnerability	https://code.vtiger.com/vtiger/vtigercrm	A-VTI-VTIG-101022/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			via the e-mail template modules. **CVE ID : CVE-2022-38335**		
Vendor: vuetifyjs					
Product: vuetify					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Sep-2022	5.4	The package vuetify from 2.0.0-beta.4 and before 2.6.10 are vulnerable to Cross-site Scripting (XSS) due to improper input sanitization in the 'eventName' function within the VCalendar component. **CVE ID : CVE-2022-25873**	https://github.com/vuetifyjs/vuetify/commit/ade1434927f55a0eccf3d54f900f24c5fa85a176	A-VUE-VUET-101022/1236
Affected Version(s): From (including) 2.0.1 Up to (excluding) 2.6.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Sep-2022	5.4	The package vuetify from 2.0.0-beta.4 and before 2.6.10 are vulnerable to Cross-site Scripting (XSS) due to improper input sanitization in the 'eventName' function within the VCalendar component. **CVE ID : CVE-2022-25873**	https://github.com/vuetifyjs/vuetify/commit/ade1434927f55a0eccf3d54f900f24c5fa85a176	A-VUE-VUET-101022/1237
Vendor: wasm3_project					
Product: wasm3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.5.0					
Uncontrolled Resource Consumption	20-Sep-2022	7.5	WASM3 v0.5.0 was discovered to contain a segmentation fault via the component op_Select_i32_srs in wasm3/source/m3_exec.h. **CVE ID : CVE-2022-39974**	N/A	A-WAS-WASM-101022/1238
Vendor: watchdog					
Product: anti-virus					
Affected Version(s): 1.4.158					
N/A	16-Sep-2022	7.8	Incorrect access control in Watchdog Anti-Virus v1.4.158 allows attackers to perform a DLL hijacking attack and execute arbitrary code via a crafted binary. **CVE ID : CVE-2022-38611**	N/A	A-WAT-ANTI-101022/1239
Vendor: wazuh					
Product: wazuh					
Affected Version(s): From (including) 3.6.1 Up to (including) 3.13.5					
N/A	28-Sep-2022	8.8	Wazuh v3.6.1 - v3.13.5, v4.0.0 - v4.2.7, and v4.3.0 - v4.3.7 were discovered to contain an authenticated remote code execution (RCE) vulnerability via	https://github.com/wazuh/wazuh/pull/14801	A-WAZ-WAZU-101022/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Active Response endpoint. **CVE ID : CVE-2022-40497**		
Affected Version(s): From (including) 4.0.0 Up to (including) 4.2.7					
N/A	28-Sep-2022	8.8	Wazuh v3.6.1 - v3.13.5, v4.0.0 - v4.2.7, and v4.3.0 - v4.3.7 were discovered to contain an authenticated remote code execution (RCE) vulnerability via the Active Response endpoint. **CVE ID : CVE-2022-40497**	https://github.com/wazuh/wazuh/pull/14801	A-WAZ-WAZU-101022/1241
Affected Version(s): From (including) 4.3.0 Up to (including) 4.3.7					
N/A	28-Sep-2022	8.8	Wazuh v3.6.1 - v3.13.5, v4.0.0 - v4.2.7, and v4.3.0 - v4.3.7 were discovered to contain an authenticated remote code execution (RCE) vulnerability via the Active Response endpoint. **CVE ID : CVE-2022-40497**	https://github.com/wazuh/wazuh/pull/14801	A-WAZ-WAZU-101022/1242
Vendor: webhelpagency					
Product: wha_crossword					
Affected Version(s): * Up to (including) 1.1.10					
Improper Neutralization of	21-Sep-2022	5.4	Multiple Authenticated (contributor+)	https://patchstack.com/database/vulnerability	A-WEB-WHA_-101022/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Stored Cross-Site Scripting (XSS) vulnerabilities in WHA Crossword plugin <= 1.1.10 at WordPress. **CVE ID : CVE-2022-36365**	/wha-crossword/wordpress-wha-crossword-plugin-1-1-10-multiple-authenticated-stored-cross-site-scripting-xss-vulnerabilities, https://wordpress.org/plugins/wha-crossword/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WHA Crossword plugin <= 1.1.10 at WordPress. **CVE ID : CVE-2022-37330**	https://patchstack.com/database/vulnerability/wha-crossword/wordpress-wha-crossword-plugin-1-1-10-authenticated-stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/wha-crossword/	A-WEB-WHA_-101022/1244
Product: wha_wordsearch					
Affected Version(s): * Up to (including) 2.0.1					
Improper Neutralization of Input During Web Page Generation	21-Sep-2022	5.4	Multiple Authenticated (contributor+) Stored Cross-Site Scripting (XSS) vulnerabilities in WHA Word Search Puzzles game	https://patchstack.com/database/vulnerability/wha-wordsearch/wordpress-word-search-puzzles-game-plugin-2-0-1-multiple-	A-WEB-WHA_-101022/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 2.0.1 at WordPress. **CVE ID : CVE-2022-36383**	authenticated-stored-cross-site-scripting-xss-vulnerabilities, https://wordpress.org/plugins/wha-wordsearch/	
Vendor: wedding_planner_project					
Product: wedding_planner					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	9.8	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the booking_id parameter at /admin/budget.php. **CVE ID : CVE-2022-38509**	N/A	A-WED-WEDD-101022/1246
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	9.8	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /wedding_details.php. **CVE ID : CVE-2022-40483**	N/A	A-WED-WEDD-101022/1247
Improper Neutralization of Special Elements used in an	26-Sep-2022	9.8	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via	N/A	A-WED-WEDD-101022/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			the booking parameter at /admin/client_edit.php. **CVE ID : CVE-2022-40484**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	9.8	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /package_detail.php. **CVE ID : CVE-2022-40485**	N/A	A-WED-WEDD-101022/1249
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	8.8	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the booking parameter at /admin/client_assign.php. **CVE ID : CVE-2022-40402**	N/A	A-WED-WEDD-101022/1250
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Sep-2022	8.8	Wedding Planner v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/select.php. **CVE ID : CVE-2022-40404**	N/A	A-WED-WEDD-101022/1251
Improper Neutralizat	26-Sep-2022	7.2	Wedding Planner v1.0 was	N/A	A-WED-WEDD-101022/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			discovered to contain a SQL injection vulnerability via the id parameter at /admin/feature_edit.php. **CVE ID : CVE-2022-40403**		
Vendor: westerndigital					
Product: wd_discovery					
Affected Version(s): * Up to (excluding) 4.4.396					
Use of a Broken or Risky Cryptographic Algorithm	19-Sep-2022	5.3	WD Discovery software executable files were signed with an unsafe SHA-1 hashing algorithm. An attacker could use this weakness to create forged certificate signatures due to the use of a hashing algorithm that is not collision-free. This could thereby impact the confidentiality of user content. This issue affects: Western Digital WD Discovery WD Discovery Desktop App versions prior to 4.4.396 on Mac; WD Discovery Desktop App versions prior to 4.4.396 on Windows.	https://www.westerndigital.com/support/product-security/wdc-22014-wd-discovery-desktop-app-version-4-4-396	A-WES-WD_D-101022/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29835		
Vendor: whatsapp					
Product: whatsapp					
Affected Version(s): * Up to (excluding) 2.22.15.9					
Integer Underflow (Wrap or Wraparound)	23-Sep-2022	7.8	An integer underflow in WhatsApp could have caused remote code execution when receiving a crafted video file. **CVE ID : CVE-2022-27492**	https://www.whatsapp.com/security/advisories/2022/	A-WHA-WHAT-101022/1254
Affected Version(s): * Up to (excluding) 2.22.16.12					
Integer Overflow or Wraparound	22-Sep-2022	9.8	An integer overflow in WhatsApp could result in remote code execution in an established video call. **CVE ID : CVE-2022-36934**	https://www.whatsapp.com/security/advisories/2022/	A-WHA-WHAT-101022/1255
Affected Version(s): * Up to (excluding) 2.22.16.2					
Integer Underflow (Wrap or Wraparound)	23-Sep-2022	7.8	An integer underflow in WhatsApp could have caused remote code execution when receiving a crafted video file. **CVE ID : CVE-2022-27492**	https://www.whatsapp.com/security/advisories/2022/	A-WHA-WHAT-101022/1256
Vendor: woobewoo					
Product: wbw_currency_switcher_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.6.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	4.8	The WBW Currency Switcher for WooCommerce WordPress plugin before 1.6.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2575**	N/A	A-WOO-WBW_-101022/1257
Vendor: wordfence					
Product: wordfence_security					
Affected Version(s): * Up to (including) 7.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	4.8	The Wordfence Security – Firewall & Malware Scan plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 7.6.0 via a setting on the options page due to insufficient escaping on the stored value. This makes it possible for authenticated users, with	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2780937%40wordfence&new=2780937%40wordfence&sfp_email=&sfph_mail=	A-WOR-WORD-101022/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges, to inject malicious web scripts into the setting that executes whenever a user accesses a page displaying the affected setting on sites running a vulnerable version. **CVE ID : CVE-2022-3144**		
Vendor: wordlift					
Product: wordlift					
Affected Version(s): * Up to (excluding) 3.37.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	4.8	The WordLift WordPress plugin before 3.37.2 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-3069**	N/A	A-WOR-WORD-101022/1259
Vendor: wordpress_ping_optimizer_project					
Product: wordpress_ping_optimizer					
Affected Version(s): * Up to (excluding) 2.35.1.3.0					
Cross-Site Request Forgery (CSRF)	19-Sep-2022	4.3	The WordPress Ping Optimizer WordPress plugin before 2.35.1.3.0 does not have CSRF check in place	https://wpscan.com/vulnerability/b1a52c7e-3422-40dd-	A-WOR-WORD-101022/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2022-1591**	af5a-ea4c622a87aa	
Vendor: wp-staging					
Product: wp_staging					
Affected Version(s): * Up to (excluding) 2.9.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	4.8	The WP STAGING WordPress plugin before 2.9.18 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2737**	N/A	A-WP--WP_S-101022/1261
Vendor: wpaffiliatemanager					
Product: affiliates_manager					
Affected Version(s): * Up to (excluding) 2.9.14					
Improper Neutralization of Formula Elements	16-Sep-2022	8	The Affiliates Manager WordPress plugin before 2.9.14 does not validate and sanitise the affiliate data, which could	N/A	A-WPA-AFFI-101022/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in a CSV File			allow users registering as affiliate to perform CSV injection attacks against an admin exporting the data **CVE ID : CVE-2022-2798**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	4.8	The Affiliates Manager WordPress plugin before 2.9.14 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-2799**	N/A	A-WPA-AFFI-101022/1263
Vendor: wpchill					
Product: cpo_shortcodes					
Affected Version(s): * Up to (including) 1.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	4.8	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CPO Shortcodes plugin <= 1.5.0 at WordPress. **CVE ID : CVE-2022-40672**	https://patchstack.com/database/vulnerability/cpo-shortcodes/wordpress-cpo-shortcodes-plugin-1-5-0-authenticated-stored-cross-site-scripting-xss-vulnerability/_s	A-WPC-CPO_-101022/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				_id=cve, https://wordpress.org/plugins/cpo-shortcodes/	
Vendor: wpexperts					
Product: post_smpt					
Affected Version(s): * Up to (excluding) 2.1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	4.8	The Post SMTP Mailer/Email Log WordPress plugin before 2.1.4 does not escape some of its settings before outputting them in the admins dashboard, allowing high privilege users to perform Cross-Site Scripting attacks against other users even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-2351**	N/A	A-WPE-POST-101022/1265
Vendor: wpvivid					
Product: migration\,_backup\,_staging					
Affected Version(s): * Up to (excluding) 0.9.76					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	4.9	The Migration, Backup, Staging WordPress plugin before 0.9.76 does not sanitise and validate a parameter before using it to read the content of a file, allowing high	https://wpscan.com/vulnerability/cb6a3304-2166-47a0-a011-4dcacaa133e5	A-WPV-MIGR-101022/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege users to read any file from the web server via a Traversal attack **CVE ID : CVE-2022-2863**		
Vendor: wp_taxonomy_import_project					
Product: wp_taxonomy_import					
Affected Version(s): * Up to (including) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	6.1	The WP Taxonomy Import WordPress plugin through 1.0.4 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-2669**	N/A	A-WP_-WP_T-101022/1267
Vendor: xbifrost					
Product: bifrost					
Affected Version(s): * Up to (excluding) 1.8.7					
Incorrect Permission Assignment for Critical Resource	26-Sep-2022	6.5	Bifrost is a middleware package which can synchronize MySQL/MariaDB binlog data to other types of databases. Versions 1.8.6-release and prior are vulnerable to authentication bypass when using HTTP basic authentication. This may allow group members	https://github.com/brokercap/Bifrost/security/advisories/GHSA-p6fh-xc6r-g5hw	A-XBI-BIFR-101022/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who only have read permissions to write requests when they are normally forbidden from doing so. Version 1.8.7-release contains a patch. There are currently no known workarounds. **CVE ID : CVE-2022-39219**		
Vendor: xdsoft					
Product: jodit_editor					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.20.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Sep-2022	6.1	Jodit Editor is a WYSIWYG editor written in pure TypeScript without the use of additional libraries. Jodit Editor is vulnerable to XSS attacks when pasting specially constructed input. This issue has not been fully patched. There are no known workarounds. **CVE ID : CVE-2022-23461**	https://securitylab.github.com/advisories/GHSL-2022-030_xdan_jodit/	A-XDS-JODI-101022/1269
Vendor: xpdfreader					
Product: xpdf					
Affected Version(s): 4.04					
Use After Free	29-Sep-2022	7.8	There is a use-after-free issue in JBIG2Stream::close	https://forum.xpdfreader.com/	A-XPD-XPDF-101022/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			() located in JBIG2Stream.cc in Xpdf 4.04. It can be triggered by sending a crafted PDF file to (for example) the pdfimages binary. It allows an attacker to cause Denial of Service or possibly have unspecified other impact. **CVE ID : CVE-2022-38222**	viewtopic.php?f=3&t=42320	
NULL Pointer Dereference	21-Sep-2022	7.8	XPDF 4.04 is vulnerable to Null Pointer Dereference in FoFiType1C.cc:2393. **CVE ID : CVE-2022-38928**	https://forum.xpdfreader.com/viewtopic.php?f=3&t=42325&sid=7b08ba9a518a99ce3c5ff40e53fc6421	A-XPD-XPDF-101022/1271
Vendor: xplodedthemes					
Product: wpide					
Affected Version(s): * Up to (including) 2.6					
Unrestricted Upload of File with Dangerous Type	21-Sep-2022	7.2	Authenticated (admin+) Arbitrary File Edit/Upload vulnerability in XplodedThemes WPide plugin <= 2.6 at WordPress. **CVE ID : CVE-2022-40217**	https://patchstack.com/database/vulnerability/wpide/wordpress-wpide-plugin-2-6-authenticated-arbitrary-file-edit-upload-vulnerability, https://wordpress.org/plugins/wpide/#developers	A-XPL-WPID-101022/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: xstream_project					
Product: xstream					
Affected Version(s): * Up to (excluding) 1.4.19					
Out-of-bounds Write	16-Sep-2022	7.5	Those using Xstream to seralize XML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40153**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=49858, https://github.com/x-stream/xstream/issues/304	A-XST-XSTR-101022/1273
Out-of-bounds Write	16-Sep-2022	7.5	Those using Xstream to serialise XML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack overflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40154**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50393, https://github.com/x-stream/xstream/issues/304	A-XST-XSTR-101022/1274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.5	Those using Xstream to serialise XML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stack overflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40155**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50428, https://github.com/x-stream/xstream/issues/304	A-XST-XSTR-101022/1275
Out-of-bounds Write	16-Sep-2022	7.5	Those using Xstream to seralize XML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40156**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50841, https://github.com/x-stream/xstream/issues/304	A-XST-XSTR-101022/1276
Affected Version(s): * Up to (including) 1.4.19					
Out-of-bounds Write	16-Sep-2022	7.5	Those using Xstream to seralize XML data may be	https://github.com/x-stream/xstream	A-XST-XSTR-101022/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40151**	/issues/304, https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47367	
Out-of-bounds Write	16-Sep-2022	7.5	Those using Xstream to seralize XML data may be vulnerable to Denial of Service attacks (DOS). If the parser is running on user supplied input, an attacker may supply content that causes the parser to crash by stackoverflow. This effect may support a denial of service attack. **CVE ID : CVE-2022-40152**	https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434, https://github.com/x-stream/xstream/issues/304	A-XST-XSTR-101022/1278
Vendor: xuxueli					
Product: xxl-job					
Affected Version(s): 2.2.0					
Improper Neutralization of Special	28-Sep-2022	9.8	XXL-JOB 2.2.0 has a Command execution	N/A	A-XUX-XXL--101022/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			vulnerability in background tasks. **CVE ID : CVE-2022-40929**		
Vendor: ydesignservices					
Product: yds_support_ticket_system					
Affected Version(s): * Up to (including) 1.0					
Cross-Site Request Forgery (CSRF)	23-Sep-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in YDS Support Ticket System plugin <= 1.0 at WordPress. **CVE ID : CVE-2022-36388**	https://wordpress.org/plugins/yds-support-ticket-system/, https://patchstack.com/database/vulnerability/yds-support-ticket-system/wordpress-yds-support-ticket-system-plugin-1-0-cross-site-request-forgery-csrf-vulnerability/_s_id=cve	A-YDE-YDS_-101022/1280
Vendor: yetiforce					
Product: yetiforce_customer_relationship_management					
Affected Version(s): * Up to (excluding) 6.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.3. **CVE ID : CVE-2022-2924**	https://github.com/yetiforcecompany/yetiforcecrm/commit/b716ecea340783b842498425faa029800bd30420, https://huntr.dev/bounties/f0f3aded-6e97-	A-YET-YETI-101022/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4cf2-980a-c90f2c6ca0e0	
Affected Version(s): * Up to (excluding) 6.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. **CVE ID : CVE-2022-3000**	https://huntr.dev/bounties/a060d3dd-6fdd-4958-82a9-364df1cb770c, https://github.com/yetiforcecompany/yetiforcecrm/commit/ebc12601495ada38495076bec12841b2477516b	A-YET-YETI-101022/1282
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. **CVE ID : CVE-2022-3004**	https://huntr.dev/bounties/461e5f8f-17cf-4be4-9149-111d0bd92d14, https://github.com/yetiforcecompany/yetiforcecrm/commit/cd82ecce44d83f1f6c10c7766bf36f3026de024a	A-YET-YETI-101022/1283
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Sep-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository yetiforcecompany/yetiforcecrm prior to 6.4.0. **CVE ID : CVE-2022-3005**	https://huntr.dev/bounties/4b144433-a979-4c4e-a627-659838acc217, https://github.com/yetiforcecompany/yetiforcecrm/commit/e55886781509fe39951fc7528347696474a17884	A-YET-YETI-101022/1284
Vendor: yimihome					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ywoa					
Affected Version(s): 6.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	8.8	ywoa v6.1 is vulnerable to SQL Injection via backend/oa/visual/exportExcel.do interface. **CVE ID : CVE-2022-38808**	N/A	A-YIM-YWOA-101022/1285
Vendor: yordam					
Product: library_automation_system					
Affected Version(s): * Up to (excluding) 19.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Sep-2022	6.1	University Library Automation System developed by Yordam Bilgi Teknolojileri before version 19.2 has an unauthenticated Reflected XSS vulnerability. This has been fixed in the version 19.2 **CVE ID : CVE-2022-2266**	https://www.usom.gov.tr/bildirim/tr-22-0637	A-YOR-LIBR-101022/1286
Vendor: Zammad					
Product: Zammad					
Affected Version(s): From (including) 5.2.0 Up to (excluding) 5.2.2					
Exposure of Resource to Wrong Sphere	27-Sep-2022	6.5	Zammad 5.2.1 is vulnerable to Incorrect Access Control. Zammad's asset handling mechanism has logic to ensure that customer users are	https://zammad.com/de/advisories/zaa-2022-09	A-ZAM-ZAMM-101022/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not able to see personal information of other users. This logic was not effective when used through a web socket connection, so that a logged-in attacker would be able to fetch personal data of other users by querying the Zammad API. This issue is fixed in , 5.2.2. **CVE ID : CVE-2022-40816**		
Incorrect Permission Assignment for Critical Resource	27-Sep-2022	4.3	Zammad 5.2.1 has a fine-grained permission model that allows to configure read-only access to tickets. However, agents were still wrongly able to perform some operations on such tickets, like adding and removing links, tags. and related answers. This issue has been fixed in 5.2.2. **CVE ID : CVE-2022-40817**	https://zammad.com/de/advisories/zaa-2022-10	A-ZAM-ZAMM-101022/1288
Vendor: zapier					
Product: code_by_zapier					
Affected Version(s): * Up to (excluding) 2022-08-17					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	21-Sep-2022	9.9	Code by Zapier before 2022-08-17 allowed intra-account privilege escalation that included execution of Python or JavaScript code. In other words, Code by Zapier was providing a customer-controlled general-purpose virtual machine that unintentionally granted full access to all users of a company's account, but was supposed to enforce role-based access control within that company's account. Before 2022-08-17, a customer could have resolved this by (in effect) using a separate virtual machine for an application that held credentials - or other secrets - that weren't supposed to be shared among all of its employees. (Multiple accounts would have been needed to operate these independent virtual machines.)	https://www.zenity.io/blog/zap escape-organization-wide-control-over-code-by-zapier/, https://www.zenity.io/blog/zap escape-vulnerability-disclosure/	A-ZAP-CODE-101022/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28802		
Vendor: zblogcn					
Product: z-blogphp					
Affected Version(s): * Up to (including) 1.7.2					
Server-Side Request Forgery (SSRF)	20-Sep-2022	9.8	A security issue was discovered in Z-BlogPHP <= 1.7.2. A Server-Side Request Forgery (SSRF) vulnerability in the zb_users/plugin/UEditor/php/action_crawler.php file allows remote attackers to force the application to make arbitrary requests via injection of arbitrary URLs into the source parameter. **CVE ID : CVE-2022-40357**	N/A	A-ZBL-Z-BL-101022/1290
Vendor: zealousweb					
Product: generate_pdf_using_contact_form_7					
Affected Version(s): * Up to (excluding) 3.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Sep-2022	4.8	The Generate PDF WordPress plugin before 3.6 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html	https://wpscan.com/vulnerability/cd8d71d1-030e-4ad4-866e-75d242883c6c	A-ZEA-GENE-101022/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed. **CVE ID : CVE-2022-3070**		
Vendor: zephyr-one					
Product: zephyr_project_manager					
Affected Version(s): * Up to (excluding) 3.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	5.4	A vulnerability, which was classified as problematic, was found in Zephyr Project Manager up to 3.2.4. Affected is an unknown function of the file /v1/tasks/create/ of the component REST Call Handler. The manipulation of the argument onanimationstart leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 3.2.5 is able to address this issue. It is recommended to upgrade the affected component. VDB-209370 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-3333**	https://wpscan.com/vulnerability/bfd8a7aa-5977-4fe5-b2fc-12bf93caf3ed	A-ZEP-ZEPH-101022/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: zephyr_project_manager_project					
Product: zephyr_project_manager					
Affected Version(s): * Up to (excluding) 3.2.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Sep-2022	9.8	The Zephyr Project Manager WordPress plugin before 3.2.5 does not sanitise and escape various parameters before using them in SQL statements via various AJAX actions available to both unauthenticated and authenticated users, leading to SQL injections **CVE ID : CVE-2022-2840**	https://wpscan.com/vulnerability/13d8be88-c3b7-4d6e-9792-c98b801ba53c	A-ZEP-ZEPH-101022/1293
Vendor: zfile					
Product: zfile					
Affected Version(s): 4.1.1					
Unrestricted Upload of File with Dangerous Type	26-Sep-2022	9.8	ZFile v4.1.1 was discovered to contain an arbitrary file upload vulnerability via the component /file/upload/1. **CVE ID : CVE-2022-40050**	N/A	A-ZFI-ZFIL-101022/1294
Vendor: Zimbra					
Product: collaboration					
Affected Version(s): 8.8.15					
Unrestricted Upload of	26-Sep-2022	9.8	An issue was discovered in	https://wiki.zimbra.com/wiki	A-ZIM-COLL-101022/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			Zimbra Collaboration (ZCS) 8.8.15 and 9.0. An attacker can upload arbitrary files through amavisd via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can lead to incorrect access to any other user accounts. Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavisd automatically prefers it over cpio. **CVE ID : CVE-2022-41352**	/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center, https://forums.zimbra.org/viewtopic.php?t=71153&p=306532	
N/A	26-Sep-2022	7.8	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.x and 9.x (e.g., 8.8.15). The Sudo configuration permits the zimbra user to execute the NGINX binary as root with arbitrary parameters. As	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-101022/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			part of its intended functionality, NGINX can load a user-defined configuration file, which includes plugins in the form of .so files, which also execute as root. **CVE ID : CVE-2022-41347**		
Affected Version(s): 9.0.0					
Unrestricted Upload of File with Dangerous Type	26-Sep-2022	9.8	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.15 and 9.0. An attacker can upload arbitrary files through amavisd via a cpio loophole (extraction to /opt/zimbra/jetty/webapps/zimbra/public) that can lead to incorrect access to any other user accounts. Zimbra recommends pax over cpio. Also, pax is in the prerequisites of Zimbra on Ubuntu; however, pax is no longer part of a default Red Hat installation after RHEL 6 (or CentOS 6). Once pax is installed, amavisd	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center, https://forums.zimbra.org/viewtopic.php?t=71153&p=306532	A-ZIM-COLL-101022/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			automatically prefers it over cpio. **CVE ID : CVE-2022-41352**		
N/A	26-Sep-2022	7.8	An issue was discovered in Zimbra Collaboration (ZCS) 8.8.x and 9.x (e.g., 8.8.15). The Sudo configuration permits the zimbra user to execute the NGINX binary as root with arbitrary parameters. As part of its intended functionality, NGINX can load a user-defined configuration file, which includes plugins in the form of .so files, which also execute as root. **CVE ID : CVE-2022-41347**	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories, https://wiki.zimbra.com/wiki/Security_Center	A-ZIM-COLL-101022/1298
Vendor: Zohocorp					
Product: manageengine_access_manager_plus					
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1300
Affected Version(s): 4.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1301
Affected Version(s): 4.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1302
Product: manageengine_pam360					
Affected Version(s): 5.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1303
Affected Version(s): 4.0					
Improper Neutralization of Special Elements used in an SQL	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600,	https://www.manageengine.com/products/passwordmanagerpro/advisory/c	A-ZOH-MANA-101022/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	ve-2022-40300.html	
Affected Version(s): 4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1305
Affected Version(s): 4.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities.	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40300		
Affected Version(s): 5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1307
Affected Version(s): 5.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1308
Affected Version(s): 5.3					
Improper Neutralization of Special	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120	https://www.manageengine.com/products/passwordmanager	A-ZOH-MANA-101022/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	pro/advisory/cve-2022-40300.html	
Affected Version(s): 5.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1310
Affected Version(s): 5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Product: manageengine_password_manager_pro					
Affected Version(s): 8.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1312
Affected Version(s): 9.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1313
Affected Version(s): 5.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1314
Affected Version(s): 6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1315
Affected Version(s): 8.1					
Improper Neutralization of Special Elements used in an SQL Command	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 7.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1317
Affected Version(s): 7.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities.	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40300		
Affected Version(s): 6.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1319
Affected Version(s): 9.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1320
Affected Version(s): 6.1					
Improper Neutralization of Special	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120	https://www.manageengine.com/products/passwordmanager	A-ZOH-MANA-101022/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	pro/advisory/cve-2022-40300.html	
Affected Version(s): 5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1322
Affected Version(s): 5.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1324
Affected Version(s): 5.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1325
Affected Version(s): 10.0					
Improper Neutralizat	16-Sep-2022	9.8	Zoho ManageEngine	https://www.manageengine.co	A-ZOH-MANA-101022/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	m/products/passwordmanagerpro/advisory/cve-2022-40300.html	
Affected Version(s): 10.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1327
Affected Version(s): 10.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 10.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1329
Affected Version(s): 10.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1330
Affected Version(s): 11.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1331
Affected Version(s): 11.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1332
Affected Version(s): 11.3					
Improper Neutralization of Special Elements used in an SQL Command	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 12.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1334
Affected Version(s): 12.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities.	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40300		
Affected Version(s): 4.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1336
Affected Version(s): 4.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1337
Affected Version(s): 4.8					
Improper Neutralization of Special	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120	https://www.manageengine.com/products/passwordmanager	A-ZOH-MANA-101022/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	pro/advisory/cve-2022-40300.html	
Affected Version(s): 6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1339
Affected Version(s): 6.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 6.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1341
Affected Version(s): 6.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1342
Affected Version(s): 6.6					
Improper Neutralizat	16-Sep-2022	9.8	Zoho ManageEngine	https://www.manageengine.co	A-ZOH-MANA-101022/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	m/products/passwordmanagerpro/advisory/cve-2022-40300.html	
Affected Version(s): 6.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1344
Affected Version(s): 6.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 7.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1346
Affected Version(s): 7.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1347
Affected Version(s): 8.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1348
Affected Version(s): 8.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1349
Affected Version(s): 8.4					
Improper Neutralization of Special Elements used in an SQL Command	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 8.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1351
Affected Version(s): 8.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities.	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40300		
Affected Version(s): 8.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1353
Affected Version(s): 9.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1354
Affected Version(s): 9.2					
Improper Neutralization of Special	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120	https://www.manageengine.com/products/passwordmanager	A-ZOH-MANA-101022/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	pro/advisory/cve-2022-40300.html	
Affected Version(s): 9.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1356
Affected Version(s): 9.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection vulnerabilities. **CVE ID : CVE-2022-40300**		
Affected Version(s): 9.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1358
Affected Version(s): 9.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1359
Affected Version(s): 9.7					
Improper Neutralizat	16-Sep-2022	9.8	Zoho ManageEngine	https://www.manageengine.co	A-ZOH-MANA-101022/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	m/products/passwordmanagerpro/advisory/cve-2022-40300.html	
Affected Version(s): 9.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Sep-2022	9.8	Zoho ManageEngine Password Manager Pro through 12120 before 12121, PAM360 through 5550 before 5600, and Access Manager Plus through 4304 before 4305 have multiple SQL injection vulnerabilities. **CVE ID : CVE-2022-40300**	https://www.manageengine.com/products/passwordmanagerpro/advisory/cve-2022-40300.html	A-ZOH-MANA-101022/1361
Vendor: Zoom					
Product: zoom_on-premise_meeting_connector_mmr					
Affected Version(s): * Up to (excluding) 4.8.20220815.130					
N/A	16-Sep-2022	8.2	Zoom On-Premise Meeting Connector MMR before version 4.8.20220815.130 contains an improper access	https://explore.zoom.us/en/trust/security/security-bulletin/	A-ZOO-ZOOM-101022/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control vulnerability. As a result, a malicious actor could obtain the audio and video feed of a meeting they were not authorized to join and cause other meeting disruptions. **CVE ID : CVE-2022-28758**		
Vendor: zoo_management_system_project					
Product: zoo_management_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	26-Sep-2022	7.2	Zoo Management System v1.0 has an arbitrary file upload vulnerability in the picture upload point of the "save_animal" file of the "Animals" module in the background management system. **CVE ID : CVE-2022-40924**	N/A	A-ZOO-ZOO_-101022/1363
Unrestricted Upload of File with Dangerous Type	26-Sep-2022	7.2	Zoo Management System v1.0 has an arbitrary file upload vulnerability in the picture upload point of the "save_event" file of the "Events" module in the background	N/A	A-ZOO-ZOO_-101022/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management system. **CVE ID : CVE-2022-40925**		
Unrestricted Upload of File with Dangerous Type	22-Sep-2022	7.2	In Zoo Management System v1.0, there is an arbitrary file upload vulnerability in the picture upload point of the "gallery" file of the "Gallery" module in the background management system. **CVE ID : CVE-2022-40932**	N/A	A-ZOO-ZOO_-101022/1365
Vendor: zutty_project					
Product: zutty					
Affected Version(s): * Up to (excluding) 0.13					
N/A	20-Sep-2022	9.8	In Zutty before 0.13, DECRQSS in text written to the terminal can achieve arbitrary code execution. **CVE ID : CVE-2022-41138**	https://bugs.gentoo.org/868495, https://github.com/tomszilagyi/zutty/commit/bde7458c60a7bafe08bbeaafbf861eb865edfa38, https://github.com/tomszilagyi/zutty/compare/0.12...0.13	A-ZUT-ZUTT-101022/1366
Vendor: zzcms					
Product: zzcms					
Affected Version(s): 2022					
Improper Neutralizat	22-Sep-2022	7.2	ZZCMS 2022 was discovered to	N/A	A-ZZC-ZZCM-101022/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			contain a SQL injection vulnerability via the component /admin/sendmailto.php?tomail=&groupid=. **CVE ID : CVE-2022-40446**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Sep-2022	7.2	ZZCMS 2022 was discovered to contain a SQL injection vulnerability via the keyword parameter at /admin/baojia_list.php. **CVE ID : CVE-2022-40447**	N/A	A-ZZC-ZZCM-101022/1368
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Sep-2022	5.3	An absolute path traversal vulnerability in ZZCMS 2022 allows attackers to obtain sensitive information via a crafted GET request sent to /one/siteinfo.php. **CVE ID : CVE-2022-40443**	N/A	A-ZZC-ZZCM-101022/1369
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Sep-2022	5.3	ZZCMS 2022 was discovered to contain a full path disclosure vulnerability via the page /admin/index.PHP? _server.	N/A	A-ZZC-ZZCM-101022/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40444		
Hardware					
Vendor: Acer					
Product: altos_t110_f3					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	H-ACE-ALTO-111022/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ap130_f2					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	H-ACE-AP13-111022/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_1600x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	H-ACE-ASPI-111022/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_1602m					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	H-ACE-ASPI-111022/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_7600u					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	H-ACE-ASPI-111022/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_mc605					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	H-ACE-ASPI-111022/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_tc-105					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	H-ACE-ASPI-111022/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_tc-120					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	H-ACE-ASPI-111022/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_u5-620					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	H-ACE-ASPI-111022/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: aspire_x1935					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	H-ACE-ASPI-111022/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_x3475					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	H-ACE-ASPI-111022/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_x3995					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	H-ACE-ASPI-111022/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_xc100					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	H-ACE-ASPI-111022/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_xc600					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	H-ACE-ASPI-111022/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_z3-615					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	H-ACE-ASPI-111022/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_b630_49					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_e430					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: veriton_e430g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	H-ACE-VERI-111022/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2110g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	H-ACE-VERI-111022/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2120g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	H-ACE-VERI-111022/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2611					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	H-ACE-VERI-111022/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2611g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	H-ACE-VERI-111022/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m4620					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m4620g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m6620g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: veriton_n2620g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	H-ACE-VERI-111022/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_n4620g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	H-ACE-VERI-111022/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_n4630g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	H-ACE-VERI-111022/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_s6620g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	H-ACE-VERI-111022/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x2611					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	H-ACE-VERI-111022/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x2611g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x4620g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x6620g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	H-ACE-VERI-111022/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: veriton_z2650g					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	H-ACE-VERI-111022/1404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Vendor: Festo					
Product: cpx-cec-c1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	20-Sep-2022	7.5	Festo control block CPX-CEC-C1 and CPX-CMXX in multiple versions allow unauthenticated, remote access to critical webpage functions which may cause a denial of service. **CVE ID : CVE-2022-3079**	https://cert.vde.com/en/advisories/VDE-2022-036	H-FES-CPX--111022/1405
Product: cpx-cmxx					
Affected Version(s): -					
Improper Privilege Management	20-Sep-2022	7.5	Festo control block CPX-CEC-C1 and CPX-CMXX in multiple versions allow unauthenticated, remote access to critical webpage functions which may cause a denial of service. **CVE ID : CVE-2022-3079**	https://cert.vde.com/en/advisories/VDE-2022-036	H-FES-CPX--111022/1406
Vendor: gavazziautomation					
Product: uwp_3.0_monitoring_gateway_and_controller					
Affected Version(s): -					
Use of Hard-coded Credentials	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to gain full access to the device. **CVE ID : CVE-2022-22522**		
Missing Authentication for Critical Function	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a missing authentication allows for full access via API. **CVE ID : CVE-2022-22526**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1408
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could utilize an improper input validation on an API-submitted parameter to execute arbitrary OS commands. **CVE ID : CVE-2022-28811**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1409
Use of Hard-coded Credentials	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials to gain SuperUser	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the device. **CVE ID : CVE-2022-28812**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	9.8	Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 was discovered to be vulnerable to a relative path traversal vulnerability which enables remote attackers to read arbitrary files and gain full control of the device. **CVE ID : CVE-2022-28814**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1411
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	9.4	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 an unauthenticated remote attacker could utilize a SQL-Injection vulnerability to gain full database access, modify users and stop services . **CVE ID : CVE-2022-22524**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1412
Improper Authentication	28-Sep-2022	7.5	An improper authentication vulnerability exists in the Carlo Gavazzi UWP3.0 in	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple versions and CPY Car Park Server in Version 2.8.3 Web-App which allows an authentication bypass to the context of an unauthorised user if free-access is disabled. **CVE ID : CVE-2022-22523**		
Improper Input Validation	28-Sep-2022	7.2	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 an remote attacker with admin rights could execute arbitrary commands due to missing input sanitization in the backup restore function **CVE ID : CVE-2022-22525**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1414
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Sep-2022	6.1	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 the Sentilo Proxy is prone to reflected XSS which only affects the Sentilo service. **CVE ID : CVE-2022-28816**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	5.3	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of an SQL-injection to gain access to a volatile temporary database with the current states of the device. **CVE ID : CVE-2022-28813**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1416
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	2.7	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 the Sentilo Proxy server was discovered to contain a SQL injection vulnerability allowing an attacker to query other tables of the Sentilo service. **CVE ID : CVE-2022-28815**	https://cert.vde.com/en/advisories/VDE-2022-029/	H-GAV-UWP_-111022/1417
Vendor: Grandstream					
Product: gds3710					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	an attacker with knowledge of user/pass of Grandstream GSD3710 in its	https://www.incibe-cert.es/en/early-warning/securit	H-GRA-GDS3-111022/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0.11.13 version, could overflow the stack since it doesn't check the param length before use the strcopy instruction. The explotation of this vulnerability may lead an attacker to execute a shell with full access. **CVE ID : CVE-2022-2025**	y-advisories/buffer-overflow-vulnerabilities-grandstream-gsd3710	
Out-of-bounds Write	23-Sep-2022	9.8	In Grandstream GSD3710 in its 1.0.11.13 version, it's possible to overflow the stack since it doesn't check the param length before using the sscanf instruction. Because of that, an attacker could create a socket and connect with a remote IP:port by opening a shell and getting full access to the system. The exploit affects daemons dbmng and logsrv that are running on ports 8000 and 8001 by default. **CVE ID : CVE-2022-2070**	https://www.incibe-cert.es/en/early-warning/security-advisories/buffer-overflow-vulnerabilities-grandstream-gsd3710	H-GRA-GDS3-111022/1419
Vendor: HP					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: apollo_4200_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1420
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1422
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HP-APOL-111022/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	hpesbhf04365en_us	
Product: apollo_4500					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1425
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1427
Product: apollo_r2000_chassis					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of	https://support.hpe.com/hpsc/	H-HP-APOL-111022/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1430
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HP-APOL-111022/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Vendor: hpe					
Product: apollo_2000_gen10_plus_system					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1433
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1435
Product: apollo_4200_gen10_plus_system					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-APOL-111022/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1438
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: apollo_4510_gen10_system					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28639		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1441
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1443
Product: apollo_6500_gen10_plus					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-HPE-APOL-111022/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	mr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1446
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: apollo_n2600_gen10_plus					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1449
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1451
Product: apollo_n2800_gen10_plus					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-APOL-111022/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28640		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1454
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: apollo_r2600_gen10					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1456
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary	https://support.hpe.com/hpsc/	H-HPE-APOL-111022/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1459
Product: apollo_r2800_gen10					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1462
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-APOL-111022/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: edgeline_e920d_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1464
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-EDGE-111022/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	n_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28637		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1467
Product: edgeline_e920t_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1469
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-EDGE-111022/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: edgeline_e920_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1472
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-EDGE-111022/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-EDGE-111022/1475
Product: integrated_lights-out_5					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-INTE-111022/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-INTE-111022/1477
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-INTE-111022/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-INTE-111022/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_bl460c_gen10_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1480
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1482
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
Product: proliant_dl110_gen10_plus_telco_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1485
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_dl160_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1488
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1490
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	hpesbhf04365en_us	
Product: proliant_dl180_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1493
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1495
Product: proliant_dl20_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1498
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dl20_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28639		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1501
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1503
Product: proliant_dl325_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-HPE-PROL-111022/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	mr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1506
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dl325_gen10_plus_v2_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1509
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1511
Product: proliant_dl325_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28640		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1514
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dl345_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1516
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1519
Product: proliant_dl360_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1522
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dl360_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1524
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-PROL-111022/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	n_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28637		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1527
Product: proliant_dl365_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1529
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dl380_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1532
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1535
Product: proliant_dl380_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1537
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dl385_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1540
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1542
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
Product: proliant_dl385_gen10_plus_v2_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1545
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_dl385_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1548
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1550
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	hpesbhf04365en_us	
Product: proliant_dl560_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1553
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1555
Product: proliant_dl580_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1558
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dx170r_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28639		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1561
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1563
Product: proliant_dx190r_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-HPE-PROL-111022/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	mr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1566
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dx220n_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1569
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1571
Product: proliant_dx325_gen10_plus_v2_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28640		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1574
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dx360_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1576
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1579
Product: proliant_dx360_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1582
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dx380_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1584
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-PROL-111022/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	n_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28637		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1587
Product: proliant_dx380_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1589
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dx385_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1592
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1595
Product: proliant_dx385_gen10_plus_v2_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1597
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_dx4200_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1600
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1602
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
Product: proliant_dx560_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1605
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_e910t_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1608
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1610
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	hpesbhf04365en_us	
Product: proliant_e910_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1613
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1615
Product: proliant_m750_server_blade					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1618
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_microserver_gen10_plus					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28639		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1621
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1623
Product: proliant_ml110_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-HPE-PROL-111022/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	mr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1626
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_ml30_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1629
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1631
Product: proliant_ml30_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28640		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1634
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_ml350_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1636
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1639
Product: proliant_xl170r_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1642
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_xl190r_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1644
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-PROL-111022/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	n_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28637		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1647
Product: proliant_xl220n_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1649
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_xl225n_gen10_plus_1u_node					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1652
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1655
Product: proliant_xl230k_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1657
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_xl270d_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1660
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1662
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-PROL-111022/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
Product: proliant_xl290n_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1665
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: proliant_xl420_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1668
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1670
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-PROL-111022/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	hpesbhf04365en_us	
Product: proliant_xl450_gen10_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1673
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1675
Product: proliant_xl645d_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of	https://support.hpe.com/hpsc/	H-HPE-PROL-111022/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1678
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: proliant_xl675d_gen10_plus_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28639		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1681
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1683
Product: proliant_xl925g_gen10_plus_1u_4-node_configure-to-order_server					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=e	H-HPE-PROL-111022/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	mr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1686
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-PROL-111022/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: storage_file_controller					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1689
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1691
Product: storage_performance_file_controller					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-STOR-111022/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	hpesbhf04365en_us	
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28640		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1694
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: storeeasy_1460_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1696
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary	https://support.hpe.com/hpsc/	H-HPE-STOR-111022/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1699
Product: storeeasy_1560_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1702
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: storeeasy_1660_expanded_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1704
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that	https://support.hpe.com/hpsc/doc/public/display?docLocale=e	H-HPE-STOR-111022/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	n_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28637		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1707
Product: storeeasy_1660_performance_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1709
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-STOR-111022/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: storeeasy_1660_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1712
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-STOR-111022/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1715
Product: storeeasy_1860_performance_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1717
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-	H-HPE-STOR-111022/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	hpesbhf04365en_us	
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security vulnerabilities. **CVE ID : CVE-2022-28638**		
Product: storeeasy_1860_storage					
Affected Version(s): -					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1720
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**		
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	H-HPE-STOR-111022/1722
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and	https://support.hpe.com/hpsc/doc/public/disp	H-HPE-STOR-111022/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	lay?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	
Vendor: Huawei					
Product: cv81-wdm_fw					
Affected Version(s): -					
Improper Input Validation	20-Sep-2022	7.5	A Huawei device has an input verification vulnerability. Successful exploitation of this vulnerability may lead to DoS attacks.Affected product versions include:CV81-WDM FW versions 01.70.49.29.46. **CVE ID : CVE-2022-37395**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220810-01-8cfecdcc-en	H-HUA-CV81-111022/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ws7200-10					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	20-Sep-2022	6.5	There is a password verification vulnerability in WS7200-10 11.0.2.13. Attackers on the LAN may use brute force cracking to obtain passwords, which may cause sensitive system information to be disclosed. **CVE ID : CVE-2022-33735**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220628-01-2eda0853-en	H-HUA-WS72-111022/1725
Vendor: iegeek					
Product: ig20					
Affected Version(s): -					
Use of Insufficiently Random Values	26-Sep-2022	6.5	ieGeek IG20 hipcam RealServer V1.0 is vulnerable to Incorrect Access Control. The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	N/A	H-IEG-IG20-111022/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38970		
Vendor: Intel					
Product: nuc_m15_laptop_kit_lapbc510					
Affected Version(s): -					
Out-of-bounds Write	20-Sep-2022	8.8	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms	https://www.ami.com/security-center/	H-INT-NUC_-111022/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: SmmSmbiosElog SHA256: 3a8acb4f9bddccb19ec3b22b22ad97963711550f76b27b606461cd5073a93b59 Module GUID: 8e61fd6b-7a8b-404f-b83f-aa90a47cabdf This issue affects: AMI Aptio 5.x. This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-40250**		
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and	https://www.ami.com/security-center/	H-INT-NUC_-111022/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: PlatformInitAdvancedPreMem SHA256: 644044fdb8daea30a7820e0f5f88dbf5cd460af72fbf70418e9d2e47efed8d9b Module GUID: EEEE611D-F78F-4FB9-B868-55907F169280 This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-26873**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	8.2	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in	https://www.ami.com/security-center/	H-INT-NUC_-111022/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: OverClockSmiHandler SHA256: a204699576e1a48ce915d9d9423380c8e4c197003baf9d17e6504f0265f3039c Module GUID: 4698C2BD-A903-410E-AD1F-5EEF3A1AE422 **CVE ID : CVE-2022-40261**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Sep-2022	7.2	An attacker with physical access can exploit this vulnerability to execute arbitrary code during DXE phase. A malicious code installed as a result of vulnerability exploitation in DXE driver could survive across an operating system (OS) boot process and runtime This issue affects: Module name: AMITSE SHA256: 288769fcb374d9280735e259c579e2dc209491f4da43b085d6aabc2d6e6ee57d Module GUID: b1da0adf-4f77-4070-a88e-bffe1c60529a This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-2154**	https://www.ami.com/security-center/	H-INT-NUC_-111022/1730
Out-of-bounds Write	20-Sep-2022	7.2	A potential attacker can write one byte by arbitrary address at the time of the PEI phase (only during S3 resume boot mode) and influence the subsequent boot stages. This can lead to the	https://www.ami.com/security-center/	H-INT-NUC_-111022/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: SbPei SHA256: d827182e5f9b7a9ff0b9d3e232f7cfac43b5237e2681e11f005be627a49283a9 Module GUID: c1fbd624-27ea-40d1-aa48-94c3dc5c7e0d **CVE ID : CVE-2022-40246**		
Product: nuc_m15_laptop_kit_lapbc710					
Affected Version(s): -					
Out-of-bounds Write	20-Sep-2022	8.8	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment	https://www.ami.com/security-center/	H-INT-NUC_-111022/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: SmmSmbiosElog SHA256: 3a8acb4f9bddccb19ec3b22b22ad97963711550f76b27b606461cd5073a93b59 Module GUID:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8e61fd6b-7a8b-404f-b83f-aa90a47cabdf This issue affects: AMI Aptio 5.x. This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-40250**		
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: PlatformInitAdvancedPreMem SHA256: 644044fdb8daea3	https://www.ami.com/security-center/	H-INT-NUC_-111022/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0a7820e0f5f88dbf5cd460af72fbf70418e9d2e47efed8d9b Module GUID: EEEE611D-F78F-4FB9-B868-55907F169280 This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-26873**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	8.2	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this	https://www.ami.com/security-center/	H-INT-NUC_-111022/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: OverClockSmiHandler SHA256: a204699576e1a48ce915d9d9423380c8e4c197003baf9d17e6504f0265f3039c Module GUID: 4698C2BD-A903-410E-AD1F-5EEF3A1AE422 **CVE ID : CVE-2022-40261**		
Out-of-bounds Write	20-Sep-2022	7.2	An attacker with physical access can exploit this vulnerability to execute arbitrary code during DXE phase. A malicious code installed as a result of vulnerability exploitation in DXE driver could survive across an operating system (OS) boot process and runtime This	https://www.ami.com/security-center/	H-INT-NUC_-111022/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Module name: AMITSE SHA256: 288769fcb374d9280735e259c579e2dc209491f4da43b085d6aabc2d6e6ee57d Module GUID: b1da0adf-4f77-4070-a88e-bffe1c60529a This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-2154**		
Out-of-bounds Write	20-Sep-2022	7.2	A potential attacker can write one byte by arbitrary address at the time of the PEI phase (only during S3 resume boot mode) and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can	https://www.ami.com/security-center/	H-INT-NUC_-111022/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be injected into the SMRAM memory. This issue affects: Module name: SbPei SHA256: d827182e5f9b7a9ff0b9d3e232f7cfac43b5237e2681e11f005be627a49283a9 Module GUID: c1fbd624-27ea-40d1-aa48-94c3dc5c7e0d **CVE ID : CVE-2022-40246**		
Product: server_board_m10jnp2sb					
Affected Version(s): -					
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can	https://www.ami.com/security-center/	H-INT-SERV-111022/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be injected into the SMRAM memory. This issue affects: Module name: S3Resume2Pei SHA256: 7bb29f05534a8a1e010443213451425098faebd45948a4642db969b19d0253fc Module GUID: 89E549B0-7CFE-449D-9BA3-10D8B2312D71 **CVE ID : CVE-2022-40262**		
Vendor: mipcm					
Product: mipc_camera					
Affected Version(s): -					
Out-of-bounds Write	26-Sep-2022	8.8	Unlimited strcpy on user input when setting a locale file leads to stack buffer overflow in mIPC camera firmware 5.3.1.2003161406. **CVE ID : CVE-2022-40784**	N/A	H-MIP-MIPC-111022/1738
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Sep-2022	8.8	Unsanitized input when setting a locale file leads to shell injection in mIPC camera firmware 5.3.1.2003161406. This allows an attacker to gain remote code execution on cameras running the firmware when	N/A	H-MIP-MIPC-111022/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim logs into a specially crafted mobile app. **CVE ID : CVE-2022-40785**		
Vendor: neoinfosys					
Product: nis-hap11ac					
Affected Version(s): -					
N/A	19-Sep-2022	9.8	This Vulnerability in NIS-HAP11AC is caused by an exposed external port for the telnet service. Remote attackers use this vulnerability to induce all attacks such as source code hijacking, remote control of the device. **CVE ID : CVE-2022-23768**	N/A	H-NEO-NIS--111022/1740
Vendor: Netgear					
Product: r7000					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncat	https://www.netgear.com/about/security/, https://www.netgear.com/support/download/?model=R7000	H-NET-R700-111022/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37235		
Out-of-bounds Write	22-Sep-2022	7.8	Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncpy. **CVE ID : CVE-2022-37234**	https://www.netgear.com/about/security/, https://www.netgear.com/support/download/?model=R7000	H-NET-R700-111022/1742
Product: wnr2000v4					
Affected Version(s): -					
Out-of-bounds Write	22-Sep-2022	9.8	Netgear N300 wireless router wnr2000v4-V1.0.0.70 was discovered to contain a stack overflow via strcpy in uhttpd. **CVE ID : CVE-2022-31937**	https://www.netgear.com/support/download/?model=WNR2000v4, https://www.netgear.com/about/security/	H-NET-WNR2-111022/1743
Out-of-bounds Write	23-Sep-2022	9.8	Netgear N300 wireless router wnr2000v4-V1.0.0.70 is vulnerable to Buffer Overflow via uhttpd. There is a stack overflow vulnerability caused by strcpy. **CVE ID : CVE-2022-37232**	https://www.netgear.com/about/security/	H-NET-WNR2-111022/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wpn824ext					
Affected Version(s): -					
Improper Validation of Integrity Check Value	20-Sep-2022	7.5	An exploitable firmware modification vulnerability was discovered on the Netgear WPN824EXT WiFi Range Extender. An attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the CRC check. A successful attack can either introduce a backdoor to the device or make the device DoS. This affects Firmware Version: 1.1.1_1.1.9. **CVE ID : CVE-2022-38955**	https://www.netgear.com/about/security/	H-NET-WPN8-111022/1745
Improper Validation of Integrity Check Value	20-Sep-2022	5.3	An exploitable firmware downgrade vulnerability was discovered on the Netgear WPN824EXT WiFi Range Extender. An attacker can conduct a MITM attack to replace the user-uploaded firmware image with an original old firmware image. This affects	https://www.netgear.com/about/security/	H-NET-WPN8-111022/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firmware 1.1.1_1.1.9 and earlier. **CVE ID : CVE-2022-38956**		
Vendor: Qualcomm					
Product: apq8009					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1747
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-APQ8-111022/1749
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1751
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Product: apq8009w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1753
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while	https://www.qualcomm.com/company/product-	H-QUA-APQ8-111022/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	security/bulletins/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1756
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1758
Product: apq8017					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1760
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-APQ8-111022/1762
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1764
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1766
Product: apq8053					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-APQ8-111022/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1768
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-APQ8-111022/1770
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1772
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1774
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1776
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1778
Product: apq8096au					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1780
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-APQ8-111022/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1782
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1784
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-APQ8-111022/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-APQ8-111022/1787
Product: aqt1000					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1788
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video due to buffer	https://www.qualcomm.com/company/produc	H-QUA-AQT1-111022/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	t-security/bulletins/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-AQT1-111022/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1791
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1793
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1795
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1797
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-AQT1-111022/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1799
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AQT1-111022/1801
Product: ar8031					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1803
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1805
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1807
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: ar8035					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1810
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1811
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1813
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1815
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-AR80-111022/1817
Product: csr8811					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-CSR8-111022/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: csra6620					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1821
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1823
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1825
Product: csra6640					
Affected Version(s): -					
Integer Overflow or	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow	https://www.qualcomm.com/company/product-	H-QUA-CSRA-111022/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1827
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1829
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-CSRA-111022/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRA-111022/1831
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	H-QUA-CSRA-111022/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Product: csrb31024					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRB-111022/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-CSRB-111022/1834
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRB-111022/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRB-111022/1836
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRB-111022/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-CSRB-111022/1838
Product: ipq5010					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in	https://www.qualcomm.com/company/product-	H-QUA-IPQ5-111022/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	security/bulletins/september-2022-bulletin	
Product: ipq5018					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ5-111022/1840
Product: ipq5028					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ5-111022/1841
Product: ipq6000					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ6-111022/1842
Product: ipq6005					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ6-111022/1843
Product: ipq6010					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ6-111022/1844
Product: ipq6018					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ6-111022/1845
Product: ipq6028					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ6-111022/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: ipq8070					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1847
Product: ipq8070a					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1848
Product: ipq8071					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1849
Product: ipq8071a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1850
Product: ipq8072					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1851
Product: ipq8072a					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1852
Product: ipq8074					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ8-111022/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: ipq8074a					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1854
Product: ipq8076					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1855
Product: ipq8076a					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1856
Product: ipq8078					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1857
Product: ipq8078a					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1858
Product: ipq8173					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-IPQ8-111022/1859
Product: ipq8174					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-IPQ8-111022/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: mdm9150					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1861
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1863
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Product: mdm9206					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1865
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1868
Product: mdm9250					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1869
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	H-QUA-MDM9-111022/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22058		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1872
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1874
Product: mdm9607					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1876
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1878
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1880
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-111022/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Product: mdm9626					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1882
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-111022/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22058		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1885
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1887
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: mdm9628					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1891
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-111022/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1893
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MDM9-111022/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: mdm9640					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1896
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1898
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1900
Product: mdm9650					
Affected Version(s): -					
Integer Overflow	16-Sep-2022	9.8	Memory corruption in	https://www.qualcomm.com/c	H-QUA-MDM9-111022/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ompany/product-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1902
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MDM9-111022/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1905
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1907
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MDM9-111022/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Product: msm8909w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1909
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MSM8-111022/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1911
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MSM8-111022/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1914
Product: msm8917					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1916
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MSM8-111022/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1918
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1920
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: msm8920					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1922
Product: msm8937					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while	https://www.qualcomm.com/company/product-	H-QUA-MSM8-111022/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	security/bulletins/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1925
Product: msm8940					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Product: msm8953					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1927
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MSM8-111022/1929
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MSM8-111022/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1931
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1933
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1935
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MSM8-111022/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1937
Product: msm8996au					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-MSM8-111022/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-MSM8-111022/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1940
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1942
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-MSM8-111022/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: pm8937					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-PM89-111022/1944
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-PM89-111022/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-PM89-111022/1946
Product: pmp8074					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-PMP8-111022/1947
Product: qca1062					
Affected Version(s): -					
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA1-111022/1948
Product: qca1064					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA1-111022/1949
Product: qca4020					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA4-111022/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA4-111022/1951
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA4-111022/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA4-111022/1953
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA4-111022/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA4-111022/1955
Product: qca4024					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA4-111022/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qca6174a					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/1959
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1961
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1963
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1965
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1967
Product: qca6175a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/1968
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1970
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca6310					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/1973
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1975
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1977
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: qca6320					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1979
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1982
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1984
Product: qca6335					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/1986
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1988
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1990
Product: qca6390					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1991
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1993
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1995
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1996
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/1998
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/1999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2001
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2003
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2004
Time-of-check	16-Sep-2022	7	Memory corruption in	https://www.qualcomm.com/c	H-QUA-QCA6-111022/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2006
Product: qca6391					
Affected Version(s): -					
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video module due to	https://www.qualcomm.com/company/produc	H-QUA-QCA6-111022/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	t-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2008
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2011
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2012
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2014
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2016
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2019
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2020
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2022
Product: qca6420					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2024
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2026
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	H-QUA-QCA6-111022/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2029
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2031
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2033
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22094		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2035
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2036
Product: qca6421					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2037
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2039
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2040
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	H-QUA-QCA6-111022/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2043
Product: qca6426					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2044
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	H-QUA-QCA6-111022/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2047
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2048
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2050
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2052
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2055
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2057
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2058
Product: qca6428					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qca6430					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2060
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2062
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2064
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2066
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2069
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2071
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2072
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: qca6431					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2074
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	H-QUA-QCA6-111022/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2076
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2078
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	H-QUA-QCA6-111022/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2080
Product: qca6436					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2082
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2084
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2086
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2088
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2090
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2092
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2094
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: qca6438					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2096
Product: qca6564					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2098
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2100
Product: qca6564a					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2102
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2104
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2106
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2109
Product: qca6564au					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2111
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2113
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2115
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2117
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2119
Product: qca6574					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2120
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2121
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2124
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2126
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2128
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2130
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Product: qca6574a					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2132
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2134
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2136
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2138
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	H-QUA-QCA6-111022/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2140
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	H-QUA-QCA6-111022/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2143
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: qca6574au					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2145
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2147
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2149
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2151
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2153
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2156
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2158
Product: qca6584					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2159
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2162
Product: qca6595					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2164
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca6595au					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2166
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2168
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2170
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2172
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2174
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2176
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2178
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Product: qca6694					
Affected Version(s): -					
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Product: qca6696					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2181
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2182
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	H-QUA-QCA6-111022/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA6-111022/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22058		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2185
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2187
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2189
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2191
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA6-111022/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA6-111022/2193
Product: qca8072					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in	https://www.qualcomm.com/company/product-	H-QUA-QCA8-111022/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	security/bulletins/september-2022-bulletin	
Product: qca8075					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2195
Product: qca8081					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2197
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2198
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA8-111022/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2200
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2201
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2203
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Product: qca8337					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2206
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2208
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2209
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA8-111022/2210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2211
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2213
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA8-111022/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca9367					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2215
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCA9-111022/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA9-111022/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2218
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2220
Product: qca9377					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2222
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA9-111022/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2224
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2226
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2228
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Product: qca9379					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2230
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCA9-111022/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2233
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2235
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca9888					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2237
Product: qca9889					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCA9-111022/2238
Product: qcm2290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM2-111022/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2240
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2242
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM2-111022/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	ns/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2244
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2247
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM2-111022/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Product: qcm4290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2251
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2253
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2255
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2257
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2259
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM4-111022/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: qcm6125					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2261
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2263
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCM6-111022/2264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Product: qcm6490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2266
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2268
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2270
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2272
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2274
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCM6-111022/2275
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-	https://www.qualcomm.com/company/produc	H-QUA-QCM6-111022/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	t-security/bulletins/september-2022-bulletin	
Product: qcn5021					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2277
Product: qcn5022					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2278
Product: qcn5024					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2279
Product: qcn5052					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2280
Product: qcn5054					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2281
Product: qcn5064					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: qcn5121					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2283
Product: qcn5122					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2284
Product: qcn5124					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2285
Product: qcn5152					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2286
Product: qcn5154					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2287
Product: qcn5164					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2288
Product: qcn5550					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN5-111022/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: qcn6023					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2290
Product: qcn6024					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2291
Product: qcn6100					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2292
Product: qcn6102					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2293
Product: qcn6112					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2294
Product: qcn6122					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2295
Product: qcn6132					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN6-111022/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: qcn7605					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCN7-111022/2297
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN7-111022/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qcn7606					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCN7-111022/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN7-111022/2300
Product: qcn9000					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: qcn9012					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2302
Product: qcn9022					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2303
Product: qcn9024					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2304
Product: qcn9070					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2305
Product: qcn9072					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2306
Product: qcn9074					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2307
Product: qcn9100					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCN9-111022/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: qcs2290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2309
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2311
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2313
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2315
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2317
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS2-111022/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: qcs405					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2319
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2321
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2323
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs410					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2326
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2328
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2330
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2332
Product: qcs4290					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2334
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2336
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2338
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2340
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2342
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption in display due to time-of-check time-	https://www.qualcomm.com/company/product-	H-QUA-QCS4-111022/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS4-111022/2344
Product: qcs603					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS6-111022/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2347
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2349
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2351
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: qcs605					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2353
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-QCS6-111022/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2355
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2357
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2360
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2361
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while	https://www.qualcomm.com/company/product-	H-QUA-QCS6-111022/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	security/bulletins/september-2022-bulletin	
Product: qcs610					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2363
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing	https://www.qualcomm.com/company/produc	H-QUA-QCS6-111022/2364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	t-security/bulletins/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2366
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2368
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2370
Product: qcs6125					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2372
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2374
Product: qcs6490					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	H-QUA-QCS6-111022/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2376
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS6-111022/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2378
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2380
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2382
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QCS6-111022/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2384
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QCS6-111022/2386
Product: qrb5165					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2388
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22092		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2390
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25670		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2392
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2394
Product: qrb5165m					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2396
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2397
Use After Free	16-Sep-2022	7.8	Memory corruption in synx	https://www.qualcomm.com/c	H-QUA-QRB5-111022/2398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2400
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2402
Product: qrb5165n					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2404
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2405
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-	https://www.qualcomm.com/company/produc	H-QUA-QRB5-111022/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2407
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	H-QUA-QRB5-111022/2408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QRB5-111022/2410
Product: qsm8350					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QSM8-111022/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QSM8-111022/2412
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QSM8-111022/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QSM8-111022/2414
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QSM8-111022/2415
Product: qualcomm215					
Affected Version(s): -					
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QUAL-111022/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2417
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-QUAL-111022/2418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2420
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2422
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2424
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-QUAL-111022/2426
Product: sa415m					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA41-111022/2427
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA41-111022/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA41-111022/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA41-111022/2430
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA41-111022/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA41-111022/2432
Product: sa515m					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA51-111022/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA51-111022/2434
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA51-111022/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA51-111022/2436
Product: sa6145p					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	H-QUA-SA61-111022/2437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2439
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2441
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2443
Product: sa6155					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2445
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2447
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2449
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2451
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA61-111022/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Product: sa6155p					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2453
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2455
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2457
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2459
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2461
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA61-111022/2463
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA61-111022/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Product: sa8155					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2465
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2467
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2469
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2471
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-111022/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa8155p					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2474
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2475
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SA81-111022/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2477
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	H-QUA-SA81-111022/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2479
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2481
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2484
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2485
Product: sa8195p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2486
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2487
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2489
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer	https://www.qualcomm.com/company/product-	H-QUA-SA81-111022/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2491
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2493
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2496
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SA81-111022/2497
Product: sc8180x\+sdx55					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SC81-111022/2498
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SC81-111022/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SC81-111022/2500
Product: sd429					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2502
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD42-111022/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2504
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD42-111022/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2506
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD42-111022/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2509
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD42-111022/2510
Product: sd439					
Affected Version(s): -					
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video module due to	https://www.qualcomm.com/company/produc	H-QUA-SD43-111022/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	t-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2512
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD43-111022/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2515
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2517
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2519
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD43-111022/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: sd450					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD45-111022/2521
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD45-111022/2522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD45-111022/2523
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD45-111022/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD45-111022/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD45-111022/2526
Product: sd460					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2528
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2530
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22095		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2532
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2534
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2536
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2538
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD46-111022/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd480					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2540
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2542
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2544
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD48-111022/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2546
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD48-111022/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2549
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD48-111022/2550
Product: sd632					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD63-111022/2551
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD63-111022/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD63-111022/2553
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD63-111022/2554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD63-111022/2555
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD63-111022/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD63-111022/2557
Product: sd660					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2559
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD66-111022/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2561
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	H-QUA-SD66-111022/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2563
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	H-QUA-SD66-111022/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Product: sd662					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2566
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2568
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2570
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2572
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2574
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2576
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd665					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2578
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2580
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2582
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2584
Time-of-check Time-of-	16-Sep-2022	7	Memory corruption in display due to	https://www.qualcomm.com/company/produc	H-QUA-SD66-111022/2585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD66-111022/2586
Product: sd670					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	H-QUA-SD67-111022/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2588
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD67-111022/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2591
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2593
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: sd675					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2595
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2597
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2599
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2601
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2603
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption in display due to time-of-check time-	https://www.qualcomm.com/company/product-	H-QUA-SD67-111022/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2605
Product: sd678					
Affected Version(s): -					
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD67-111022/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2607
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD67-111022/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2609
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	H-QUA-SD67-111022/2610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2611
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	H-QUA-SD67-111022/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2614
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD67-111022/2616
Product: sd680					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2618
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2620
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22095		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2622
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2624
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2626
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD68-111022/2627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd690_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2630
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2632
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2634
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2636
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2638
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd695					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2640
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2642
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2644
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD69-111022/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2647
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD69-111022/2648
Product: sd710					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD71-111022/2651
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2653
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2655
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2657
Product: sd712					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD71-111022/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd720g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2660
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2662
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2664
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2666
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD72-111022/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2668
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD72-111022/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd730					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2670
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2672
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2674
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD73-111022/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2676
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	H-QUA-SD73-111022/2677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2679
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD73-111022/2680
Product: sd750g					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2683
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2685
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2687
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2689
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2691
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD75-111022/2692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd765					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2695
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2697
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2699
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2701
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2703
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2705
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2707
Product: sd765g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2709
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2711
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2712
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-	https://www.qualcomm.com/company/produc	H-QUA-SD76-111022/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2714
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2717
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2719
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2720
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD76-111022/2721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: sd768					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2722
Product: sd768g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2725
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2727
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2728
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2730
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	H-QUA-SD76-111022/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2733
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2734
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD76-111022/2735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD76-111022/2736
Product: sd778					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD77-111022/2737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Product: sd778g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2738
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD77-111022/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2741
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2742
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD77-111022/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2745
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2747
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2748
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD77-111022/2749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd780					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2750
Product: sd780g					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	H-QUA-SD78-111022/2751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2752
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD78-111022/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2754
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use	https://www.qualcomm.com/company/produc	H-QUA-SD78-111022/2755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	t-security/bulletins/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2756
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2758
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD78-111022/2759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2760
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD78-111022/2761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2762
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD78-111022/2763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd7c					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD7C-111022/2764
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD7C-111022/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD7C-111022/2766
Product: sd820					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue	https://www.qualcomm.com/company/produc	H-QUA-SD82-111022/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	t-security/bulletins/july-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD82-111022/2768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD82-111022/2769
Product: sd835					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD83-111022/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD83-111022/2771
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD83-111022/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD83-111022/2773
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD83-111022/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD83-111022/2775
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD83-111022/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Product: sd845					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD84-111022/2777
Use After Free	26-Sep-2022	7.8	Memory corruption due to	https://www.qualcomm.com/c	H-QUA-SD84-111022/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ompany/product-security/bulletins/july-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD84-111022/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD84-111022/2780
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD84-111022/2781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD84-111022/2782
Product: sd850					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2784
Product: sd855					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2785
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SD85-111022/2787
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2789
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2791
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2793
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2795
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD85-111022/2797
Product: sd865_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2799
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2801
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2803
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2805
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2807
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2809
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2811
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD86-111022/2813
Product: sd870					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2815
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2817
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2818
Use After Free	16-Sep-2022	7.8	Memory corruption in synx	https://www.qualcomm.com/c	H-QUA-SD87-111022/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	ompany/product-security/bulletins/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2820
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD87-111022/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2822
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD87-111022/2823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2825
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2827
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD87-111022/2828
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-	https://www.qualcomm.com/company/produc	H-QUA-SD87-111022/2829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	t-security/bulletins/september-2022-bulletin	
Product: sd888					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2830
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD88-111022/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2833
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2834
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD88-111022/2835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2836
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD88-111022/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2839
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2840
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2842
Product: sd888_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2844
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25708		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2846
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2848
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2849
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2851
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2853
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD88-111022/2854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2856
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2857
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD88-111022/2859
Product: sdm429w					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM4-111022/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SDM4-111022/2861
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	H-QUA-SDM4-111022/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM4-111022/2863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM4-111022/2864
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM4-111022/2865
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while	https://www.qualcomm.com/company/product-	H-QUA-SDM4-111022/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	security/bulletins/september-2022-bulletin	
Product: sdm630					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM6-111022/2867
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SDM6-111022/2868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM6-111022/2869
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SDM6-111022/2870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM6-111022/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDM6-111022/2872
Product: sdw2500					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDW2-111022/2873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SDW2-111022/2874
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDW2-111022/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDW2-111022/2876
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDW2-111022/2877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDW2-111022/2878
Product: sdx12					
Affected Version(s): -					
Integer Overflow or	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to	https://www.qualcomm.com/company/product-	H-QUA-SDX1-111022/2879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX1-111022/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25670		
Product: sdx20					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2881
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SDX2-111022/2883
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2885
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2887
Product: sdx24					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SDX2-111022/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2890
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX2-111022/2891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Product: sdx50m					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2894
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2896
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2898
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sdx55					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2902
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2904
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22095		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2906
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2908
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2910
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2912
Product: sdx55m					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2914
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2916
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2918
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2920
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2922
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2924
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2926
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX5-111022/2928
Product: sdx65					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2930
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2932
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2933
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2935
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDX6-111022/2937
Product: sdxr1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2938
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-SDXR-111022/2939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2940
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2942
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2944
Product: sdxr2_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2946
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2948
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SDXR-111022/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2950
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2952
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2954
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2956
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2958
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SDXR-111022/2959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd_636					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2960
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2962
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2964
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2966
Product: sd_675					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2968
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2970
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD_6-111022/2971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2972
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD_6-111022/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2975
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_6-111022/2977
Product: sd_8cx					
Affected Version(s): -					
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2979
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Product: sd_8cx_gen2					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2981
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2983
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2985
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SD_8-111022/2986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	ns/september-2022-bulletin	
Product: sd_8cx_gen3					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2987
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: sd_8_gen1_5g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2989
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	H-QUA-SD_8-111022/2990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2991
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2993
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2995
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2996
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2998
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/2999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3000
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3002
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3004
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3006
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SD_8-111022/3007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: sm4125					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3008
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3010
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3012
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3014
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3016
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM41-111022/3018
Product: sm6250					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3020
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3022
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3024
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	H-QUA-SM62-111022/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3027
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3028
Product: sm6250p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3029
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3031
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3033
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM62-111022/3035
Product: sm7250p					
Affected Version(s): -					
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM72-111022/3036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3037
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM72-111022/3038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3039
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in	https://www.qualcomm.com/company/product-	H-QUA-SM72-111022/3040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3041
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3043
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3045
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM72-111022/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3047
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3049
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM72-111022/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sm7315					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3051
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3053
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3055
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3057
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3059
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3061
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3063
Product: sm7325p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3064
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	H-QUA-SM73-111022/3065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3067
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3068
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in	https://www.qualcomm.com/company/product-	H-QUA-SM73-111022/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3071
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3073
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM73-111022/3074
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM73-111022/3075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: sm7450					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3076
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3078
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3080
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22081		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3082
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3083
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3085
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3087
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3089
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3091
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3093
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM74-111022/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: sm8475					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3097
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3099
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3100
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3102
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3104
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3106
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3108
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3109
Time-of-check Time-of-	16-Sep-2022	7	Memory corruption in display due to	https://www.qualcomm.com/company/produc	H-QUA-SM84-111022/3110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3111
Product: sm8475p					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	H-QUA-SM84-111022/3112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3113
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM84-111022/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3116
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3117
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3119
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3120
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3122
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3124
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SM84-111022/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3126
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SM84-111022/3128
Product: sw5100					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3130
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3132
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22081		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3134
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3136
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3138
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3140
Product: sw5100p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3141
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	H-QUA-SW51-111022/3142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3144
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3145
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-SW51-111022/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3147
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3149
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3151
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-SW51-111022/3152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcd9326					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3155
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCD9-111022/3156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3157
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3159
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3161
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3163
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3165
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption in display due to time-of-check time-	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	security/bulletins/september-2022-bulletin	
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3167
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcd9330					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3169
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCD9-111022/3170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3172
Product: wcd9335					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3173
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3175
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3178
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3180
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3182
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3184
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3186
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcd9340					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCD9-111022/3190
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3192
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3194
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3197
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3198
Product: wcd9341					
Affected Version(s): -					
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3200
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3203
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3205
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3207
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3209
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3211
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3213
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3215
Product: wcd9360					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3216
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3218
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	H-QUA-WCD9-111022/3219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Product: wcd9370					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3222
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	security/bulletins/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3225
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3226
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3228
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3229
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to	https://www.qualcomm.com/company/produc	H-QUA-WCD9-111022/3230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3231
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3233
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3235
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3237
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3239
Product: wcd9371					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3241
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3243
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3245
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	security/bulletins/september-2022-bulletin	
Product: wcd9375					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3247
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3249
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3251
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3253
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3254
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3256
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3258
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3260
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3262
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3264
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3266
Product: wcd9380					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3268
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3269
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3271
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3273
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3274
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3276
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25693		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3278
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3280
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3282
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3284
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3286
Product: wcd9385					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3288
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3289
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCD9-111022/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3292
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3293
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3295
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3296
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to	https://www.qualcomm.com/company/produc	H-QUA-WCD9-111022/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3298
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3300
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3302
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	H-QUA-WCD9-111022/3303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3304
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCD9-111022/3306
Product: wcn3610					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3308
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3310
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3312
Product: wcn3615					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3314
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3316
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3318
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3320
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3322
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3324
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn3620					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3326
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3328
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3331
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3332
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while	https://www.qualcomm.com/company/product-	H-QUA-WCN3-111022/3333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	security/bulletins/september-2022-bulletin	
Product: wcn3660					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3334
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue	https://www.qualcomm.com/company/produc	H-QUA-WCN3-111022/3335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	t-security/bulletins/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3337
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3339
Product: wcn3660b					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3341
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3343
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3345
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3347
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3349
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3351
Product: wcn3680					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3353
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3355
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3357
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-	https://www.qualcomm.com/company/product-	H-QUA-WCN3-111022/3358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	security/bulletins/september-2022-bulletin	
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3359
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn3680b					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3361
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3363
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3365
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3367
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3369
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3371
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn3910					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3375
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3377
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3379
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3381
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3383
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: wcn3950					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3385
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3387
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3389
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3391
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3393
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	H-QUA-WCN3-111022/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3396
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3397
Product: wcn3980					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3398
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3399
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3402
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3404
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3405
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3407
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3409
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	H-QUA-WCN3-111022/3410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3412
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3414
Product: wcn3988					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3415
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	H-QUA-WCN3-111022/3416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3418
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3419
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3421
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3423
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3425
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3427
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3429
Product: wcn3990					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3431
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WCN3-111022/3432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3434
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3436
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3438
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3440
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3442
Product: wcn3991					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3444
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3446
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3448
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3450
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3452
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3454
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3456
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3458
Product: wcn3998					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3459
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	H-QUA-WCN3-111022/3460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3461
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3464
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3465
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3467
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3469
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3472
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3474
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3475
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN3-111022/3476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: wcn3999					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3479
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3481
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN3-111022/3483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Product: wcn6740					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3484
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3486
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3488
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3490
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3492
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3494
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3496
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3497
Product: wcn6750					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3498
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3500
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3501
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN6-111022/3502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3503
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22089		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3505
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3506
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free	https://www.qualcomm.com/company/product-	H-QUA-WCN6-111022/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3508
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3510
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3512
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN6-111022/3513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3514
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3516
Product: wcn6850					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3518
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3519
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing	https://www.qualcomm.com/company/produc	H-QUA-WCN6-111022/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	t-security/bulletins/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3522
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3523
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22095		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3525
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3527
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3529
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3531
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3533
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: wcn6851					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3535
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3537
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3538
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	H-QUA-WCN6-111022/3539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3540
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3542
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3544
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3546
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3548
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3550
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3552
Product: wcn6855					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3554
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3555
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN6-111022/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3558
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3559
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3561
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3562
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3564
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3567
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3569
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3570
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WCN6-111022/3571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: wcn6856					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3572
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3574
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3576
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22081		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3578
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3579
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3581
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3583
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3585
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3587
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3589
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN6-111022/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: wcn7850					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3593
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3594
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	H-QUA-WCN7-111022/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3596
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3598
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3600
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	H-QUA-WCN7-111022/3601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3602
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3604
Product: wcn7851					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3608
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3610
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3611
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3613
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3614
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	H-QUA-WCN7-111022/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3616
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	H-QUA-WCN7-111022/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3619
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3621
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WCN7-111022/3622
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-	https://www.qualcomm.com/company/produc	H-QUA-WCN7-111022/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	t-security/bulletins/september-2022-bulletin	
Product: wsa8810					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3626
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WSA8-111022/3627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3628
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	H-QUA-WSA8-111022/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3630
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3632
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3634
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3636
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-	https://www.qualcomm.com/company/product-	H-QUA-WSA8-111022/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3638
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-111022/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3640
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3642
Product: wsa8815					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3644
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	H-QUA-WSA8-111022/3646
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3648
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22092		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3650
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3652
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3654
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3656
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3658
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3660
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3661
Product: wsa8830					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3662
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3664
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3665
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-111022/3666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3667
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22089		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3669
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3670
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3672
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3674
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3676
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3678
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3680
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: wsa8832					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3682
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3684
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3685
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	H-QUA-WSA8-111022/3686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3687
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3689
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3691
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3692
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3694
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-111022/3695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3697
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3698
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3700
Product: wsa8835					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3702
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25708		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3704
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3706
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3707
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3709
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3711
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3712
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3714
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	H-QUA-WSA8-111022/3715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3717
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3718
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	H-QUA-WSA8-111022/3719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	H-QUA-WSA8-111022/3720
Vendor: Realtek					
Product: rtl8195am					
Affected Version(s): -					
N/A	27-Sep-2022	7.5	On Realtek RTL8195AM devices before 284241d70308ff2519e40afd7b284ba	https://www.realtek.com/en	H-REA-RTL8-111022/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			892c730a3, the timer task can be locked when there are frequent and continuous Wi-Fi connection failures for the Soft AP mode. **CVE ID : CVE-2022-34326**		
Vendor: Sony					
Product: playstation_4					
Affected Version(s): -					
Out-of-bounds Write	28-Sep-2022	6.8	A vulnerability was found in Sony PS4 and PS5. It has been classified as critical. This affects the function UVFAT_readupcase table of the component exFAT Handler. The manipulation of the argument dataLength leads to heap-based buffer overflow. It is possible to launch the attack on the physical device. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-209679. **CVE ID : CVE-2022-3349**	N/A	H-SON-PLAY-111022/3722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: playstation_5					
Affected Version(s): -					
Out-of-bounds Write	28-Sep-2022	6.8	A vulnerability was found in Sony PS4 and PS5. It has been classified as critical. This affects the function UVFAT_readupcase table of the component exFAT Handler. The manipulation of the argument dataLength leads to heap-based buffer overflow. It is possible to launch the attack on the physical device. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-209679. **CVE ID : CVE-2022-3349**	N/A	H-SON-PLAY-111022/3723
Vendor: tacitine					
Product: en6200-prime_quad-100					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to	https://tacitine.com/newdownload/CVE-2022-40628.pdf	H-TAC-EN62-111022/3724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.20.1 (inclusive), due to improper control of code generation in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to execute arbitrary commands on the targeted device. **CVE ID : CVE-2022-40628**		
Session Fixation	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper session management in the Tacitine Firewall web-based management	https://tacitine.com/newdownload/CVE-2022-40630.pdf	H-TAC-EN62-111022/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to perform session fixation on the targeted device. **CVE ID : CVE-2022-40630**		
N/A	23-Sep-2022	7.5	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to insecure design in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the	https://tacitine.com/newdownload/CVE-2022-40629.pdf	H-TAC-EN62-111022/3726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to view sensitive information on the targeted device. **CVE ID : CVE-2022-40629**		
Product: en6200-prime_quad-35					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper control of code generation in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an	https://tacitine.com/newdownload/CVE-2022-40628.pdf	H-TAC-EN62-111022/3727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to execute arbitrary commands on the targeted device. **CVE ID : CVE-2022-40628**		
Session Fixation	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper session management in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to perform session fixation on the targeted device. **CVE ID : CVE-2022-40630**	https://tacitine.com/newdownload/CVE-2022-40630.pdf	H-TAC-EN62-111022/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	7.5	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to insecure design in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to view sensitive information on the targeted device. **CVE ID : CVE-2022-40629**	https://tacitine.com/newdownload/CVE-2022-40629.pdf	H-TAC-EN62-111022/3729
Vendor: Tenda					
Product: ac15					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 V15.03.05.19 contained a stack overflow via the	N/A	H-TEN-AC15-111022/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function fromAddressNat. **CVE ID : CVE-2022-40851**		
Product: ac18					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC18 router contained a stack overflow vulnerability in /goform/fast_setting_wifi_set **CVE ID : CVE-2022-40854**	N/A	H-TEN-AC18-111022/3731
Out-of-bounds Write	23-Sep-2022	7.2	Tenda AC18 router V15.03.05.19 contains a stack overflow vulnerability in the formSetQosBand->FUN_0007db78 function with the request /goform/SetNetControlList/ **CVE ID : CVE-2022-40861**	N/A	H-TEN-AC18-111022/3732
Product: ac21					
Affected Version(s): -					
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: formSetVirtualSer. **CVE ID : CVE-2022-40067**	N/A	H-TEN-AC21-111022/3733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: formSetQosBand. **CVE ID : CVE-2022-40068**	N/A	H-TEN-AC21-111022/3734
Out-of-bounds Write	19-Sep-2022	7.5	]Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: fromSetSysTime. **CVE ID : CVE-2022-40069**	N/A	H-TEN-AC21-111022/3735
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via bin/httpd, function: formSetFirewallCfg . **CVE ID : CVE-2022-40070**	N/A	H-TEN-AC21-111022/3736
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, formSetDeviceName. **CVE ID : CVE-2022-40071**	N/A	H-TEN-AC21-111022/3737
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via	N/A	H-TEN-AC21-111022/3738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/bin/httpd, function: setSmartPowerManagement. **CVE ID : CVE-2022-40072**		
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, saveParentControlInfo. **CVE ID : CVE-2022-40073**	N/A	H-TEN-AC21-111022/3739
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, setSchedWifi. **CVE ID : CVE-2022-40074**	N/A	H-TEN-AC21-111022/3740
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, form_fast_setting_wifi_set. **CVE ID : CVE-2022-40075**	N/A	H-TEN-AC21-111022/3741
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: fromSetWifiGusetBasic.	N/A	H-TEN-AC21-111022/3742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40076		
Product: i9					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Sep-2022	9.8	Tenda i9 v1.0.0.8(3828) was discovered to contain a command injection vulnerability via the FormexeCommand function. **CVE ID : CVE-2022-40100**	N/A	H-TEN-I9-111022/3743
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formWifiMacFilterSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40101**	N/A	H-TEN-I9-111022/3744
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formwrlSSIDset function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	N/A	H-TEN-I9-111022/3745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40102		
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formwrlSSIDget function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40104**	N/A	H-TEN-I9-111022/3746
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formWifiMacFilterGet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40105**	N/A	H-TEN-I9-111022/3747
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the set_local_time function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string.	N/A	H-TEN-I9-111022/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40106		
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formexeCommand function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40107**	N/A	H-TEN-I9-111022/3749
Out-of-bounds Write	23-Sep-2022	5.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formSetAutoPing function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40103**	N/A	H-TEN-I9-111022/3750
Product: rx9_pro					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Tenda RX9_Pro V22.03.02.10 is vulnerable to Buffer Overflow via httpd/setMacFilterCfg. **CVE ID : CVE-2022-38829**	N/A	H-TEN-RX9_-111022/3751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Tenda RX9_Pro V22.03.02.10 is vulnerable to Buffer Overflow via httpd/setIPv6Status. **CVE ID : CVE-2022-38830**	N/A	H-TEN-RX9_-111022/3752
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Tenda RX9_Pro V22.03.02.10 is vulnerable to Buffer Overflow via httpd/SetNetControlList **CVE ID : CVE-2022-38831**	N/A	H-TEN-RX9_-111022/3753
Product: tx3					
Affected Version(s): -					
Out-of-bounds Write	28-Sep-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11 is vulnerable to stack overflow via compare_parentcontrol_time. **CVE ID : CVE-2022-40942**	N/A	H-TEN-TX3-111022/3754
Product: w20e					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 contains a stack overflow in the function formSetPortMapping with post request 'goform/setPortMapping/'. This	N/A	H-TEN-W20E-111022/3755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) or Remote Code Execution (RCE) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters. **CVE ID : CVE-2022-40855**		
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formSetDebugCfg with request /goform/setDebugCfg/ **CVE ID : CVE-2022-40866**	N/A	H-TEN-W20E-111022/3756
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formIPMacBindDel	N/A	H-TEN-W20E-111022/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the request /goform/delIpMacBind/ **CVE ID : CVE-2022-40867**		
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formDelDhcpRule with the request /goform/delDhcpRules/ **CVE ID : CVE-2022-40868**	N/A	H-TEN-W20E-111022/3758
Vendor: Tendacn					
Product: ac15					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 router V15.03.05.19 contains a stack overflow via the list parameter at /goform/fast_setting_wifi_set **CVE ID : CVE-2022-40853**	N/A	H-TEN-AC15-111022/3759
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 router V15.03.05.19 contains a stack overflow vulnerability in the function formSetQosBand->FUN_0007dd20 with request	N/A	H-TEN-AC15-111022/3760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/SetNetControlList **CVE ID : CVE-2022-40860**		
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 router V15.03.05.19 contains stack overflow vulnerability in the function fromNatStaticSetting with the request /goform/NatStaticSetting **CVE ID : CVE-2022-40862**	N/A	H-TEN-AC15-111022/3761
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function setSmartPowerManagement with the request /goform/PowerSaveSet **CVE ID : CVE-2022-40864**	N/A	H-TEN-AC15-111022/3762
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain heap overflow vulnerabilities in the function setSchedWifi with the request /goform/openSchedWifi/	N/A	H-TEN-AC15-111022/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40865		
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function fromDhcpListClient with a combined parameter "list*" ("%s%d","list"). **CVE ID : CVE-2022-40869**	N/A	H-TEN-AC15-111022/3764
Product: ac18					
Affected Version(s): -					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 router V15.03.05.19 contains stack overflow vulnerability in the function fromNatStaticSetting with the request /goform/NatStaticSetting **CVE ID : CVE-2022-40862**	N/A	H-TEN-AC18-111022/3765
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function setSmartPowerManagement with the request	N/A	H-TEN-AC18-111022/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/PowerSaveSet **CVE ID : CVE-2022-40864**		
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain heap overflow vulnerabilities in the function setSchedWifi with the request /goform/openSchedWifi/ **CVE ID : CVE-2022-40865**	N/A	H-TEN-AC18-111022/3767
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function fromDhcpListClient with a combined parameter "list*" ("%s%d","list"). **CVE ID : CVE-2022-40869**	N/A	H-TEN-AC18-111022/3768
Vendor: Tesla					
Product: model_3					
Affected Version(s): -					
Authentication Bypass by Spoofing	16-Sep-2022	5.3	Tesla Model 3 V11.0(2022.4.5.16b701552d7a6) Tesla mobile app v4.23 is vulnerable to Authentication Bypass by spoofing. Tesla	N/A	H-TES-MODE-111022/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Model 3's Phone Key authentication is vulnerable to Man-in-the-middle attacks in the BLE channel. It allows attackers to open a door and drive the car away by leveraging access to a legitimate Phone Key. **CVE ID : CVE-2022-37709**		
Vendor: totolink					
Product: t6					
Affected Version(s): 3					
Use of Hard-coded Credentials	16-Sep-2022	9.8	In TOTOLINK T6 V4.1.5cu.709_B20210518, there is a hard coded password for root in /etc/shadow.sample. **CVE ID : CVE-2022-38823**	N/A	H-TOT-T6-111022/3770
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Sep-2022	9.8	In TOTOLINK T6 V4.1.5cu.709_B20210518, there is an execute arbitrary command in cstecgi.cgi. **CVE ID : CVE-2022-38826**	N/A	H-TOT-T6-111022/3771
Buffer Copy without Checking	16-Sep-2022	9.8	TOTOLINK T6 V4.1.5cu.709_B20210518 is vulnerable to	N/A	H-TOT-T6-111022/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Buffer Overflow via cstecgi.cgi **CVE ID : CVE-2022-38827**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Sep-2022	9.8	TOTOLINK T6 V4.1.5cu.709_B20210518 is vulnerable to command injection via cstecgi.cgi **CVE ID : CVE-2022-38828**	N/A	H-TOT-T6-111022/3773
Vendor: Tp-link					
Product: archer_ax10_v1					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	28-Sep-2022	8.8	TP Link Archer AX10 V1 Firmware Version 1.3.1 Build 20220401 Rel. 57450(5553) was discovered to allow authenticated attackers to execute arbitrary code via a crafted backup file. **CVE ID : CVE-2022-40486**	N/A	H-TP--ARCH-111022/3774
Vendor: ZTE					
Product: zxa10_b700v7					
Affected Version(s): -					
Improper Link Resolution Before File Access	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**		
Product: zxa10_b710c-a12					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3776
Product: zxa10_b710s2-a19					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			type, which affects normal use of system. **CVE ID : CVE-2022-23144**		
Product: zxa10_b766v2					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3778
Product: zxa10_b76hv3					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zxa10_b800v2					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3780
Product: zxa10_b836ct-a15					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3781
Product: zxa10_b860av2.1					
Affected Version(s): -					
Improper Link Resolution	23-Sep-2022	9.1	There is a broken access control vulnerability in	https://support.zte.com.cn/support/news/Loo	H-ZTE-ZXA1-111022/3782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	pholeInfoDetail.aspx?newsId=1026224	
Product: zxa10_b860h					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3783
Product: zxa10_b866v2-h					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**		
Product: zxa10_b866v5-w10					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3785
Product: zxa10_b960gv1					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			normal use of system. **CVE ID : CVE-2022-23144**		
Product: zxa10_s100v					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3787
Product: zxa10_s200a					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zxa10_s200t					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	H-ZTE-ZXA1-111022/3789
Vendor: Zyxel					
Product: gs1900-10hp					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web administration interface. **CVE ID : CVE-2022-34746**		
Product: gs1900-16					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3791
Product: gs1900-24					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-GS19-111022/3792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	
Product: gs1900-24e					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web administration interface. **CVE ID : CVE-2022-34746**		
Product: gs1900-24ep					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3794
Product: gs1900-24hpv2					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-GS19-111022/3795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	
Product: gs1900-48					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web administration interface. **CVE ID : CVE-2022-34746**		
Product: gs1900-48hpv2					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3797
Product: gs1900-8					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-GS19-111022/3798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	
Product: gs1900-8hp					
Affected Version(s): -					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	H-ZYX-GS19-111022/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web administration interface. **CVE ID : CVE-2022-34746**		
Operating System					
Vendor: Acer					
Product: altos_t110_f3_firmware					
Affected Version(s): * Up to (excluding) p13					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire	http://acer.com	O-ACE-ALTO-121022/3800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30426		
Product: ap130_f2_firmware					
Affected Version(s): * Up to (excluding) p04					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire	http://acer.com	O-ACE-AP13-121022/3801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_1600x_firmware					
Affected Version(s): * Up to (excluding) p11.a3l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	O-ACE-ASPI-121022/3802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_1602m_firmware					
Affected Version(s): * Up to (excluding) p11.a3l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	O-ACE-ASPI-121022/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_7600u_firmware					
Affected Version(s): * Up to (excluding) p11.a4					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	O-ACE-ASPI-121022/3804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_mc605_firmware					
Affected Version(s): * Up to (excluding) p11.a4l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	O-ACE-ASPI-121022/3805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_tc-105_firmware					
Affected Version(s): * Up to (excluding) p12.b0l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	O-ACE-ASPI-121022/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_tc-120_firmware					
Affected Version(s): * Up to (excluding) p11-a4					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	O-ACE-ASPI-121022/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_u5-620_firmware					
Affected Version(s): * Up to (excluding) p11.a1					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	O-ACE-ASPI-121022/3808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: aspire_x1935_firmware					
Affected Version(s): * Up to (excluding) p11.a3l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	O-ACE-ASPI-121022/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_x3475_firmware					
Affected Version(s): * Up to (excluding) p11.a3l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	O-ACE-ASPI-121022/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_x3995_firmware					
Affected Version(s): * Up to (excluding) p11.a3l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	O-ACE-ASPI-121022/3811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_xc100_firmware					
Affected Version(s): * Up to (excluding) p11.b3					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	O-ACE-ASPI-121022/3812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_xc600_firmware					
Affected Version(s): * Up to (excluding) p11.a4					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	O-ACE-ASPI-121022/3813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: aspire_z3-615_firmware					
Affected Version(s): * Up to (excluding) p11.a2l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	O-ACE-ASPI-121022/3814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_b630_49_firmware					
Affected Version(s): * Up to (excluding) aap02sr					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_e430g_firmware					
Affected Version(s): * Up to (excluding) p21.a1					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: veriton_e430_firmware					
Affected Version(s): * Up to (excluding) p11.a4					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	O-ACE-VERI-121022/3817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2110g_firmware					
Affected Version(s): * Up to (excluding) p21.a3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	O-ACE-VERI-121022/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2120g_firmware					
Affected Version(s): * Up to (excluding) p11-a3					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	O-ACE-VERI-121022/3819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2611g_firmware					
Affected Version(s): * Up to (excluding) p11-b0l					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	O-ACE-VERI-121022/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m2611_firmware					
Affected Version(s): * Up to (excluding) p11.b0					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	O-ACE-VERI-121022/3821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m4620g_firmware					
Affected Version(s): * Up to (excluding) p21.a3					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m4620_firmware					
Affected Version(s): * Up to (excluding) p21.a3					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_m6620g_firmware					
Affected Version(s): * Up to (excluding) p21.a0					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: veriton_n2620g_firmware					
Affected Version(s): * Up to (excluding) p21.b0					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	O-ACE-VERI-121022/3825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_n4620g_firmware					
Affected Version(s): * Up to (excluding) p11.a2l					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1	http://acer.com	O-ACE-VERI-121022/3826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_n4630g_firmware					
Affected Version(s): * Up to (excluding) p21.b0					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI	http://acer.com	O-ACE-VERI-121022/3827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_s6620g_firmware					
Affected Version(s): * Up to (excluding) p11.a1					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege	http://acer.com	O-ACE-VERI-121022/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x2611g_firmware					
Affected Version(s): * Up to (excluding) p11.a4					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110	http://acer.com	O-ACE-VERI-121022/3829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x2611_firmware					
Affected Version(s): * Up to (excluding) p11.a4					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <=		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x4620g_firmware					
Affected Version(s): * Up to (excluding) p11.a3					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Product: veriton_x6620g_firmware					
Affected Version(s): * Up to (excluding) p11.a3					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire	http://acer.com	O-ACE-VERI-121022/3832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4 (latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: veriton_z2650g_firmware					
Affected Version(s): * Up to (excluding) p21.a1					
Out-of-bounds Write	23-Sep-2022	7.8	There is a stack buffer overflow vulnerability, which could lead to arbitrary code execution in UEFI DXE driver on some Acer products. An attack could exploit this vulnerability to escalate privilege from ring 3 to ring 0, and hijack control flow during UEFI DXE execution. This affects Altos T110 F3 firmware version <= P13 (latest) and AP130 F2 firmware version <= P04 (latest) and Aspire 1600X firmware version <= P11.A3L (latest) and Aspire 1602M firmware version <= P11.A3L (latest) and Aspire 7600U firmware version <= P11.A4 (latest) and Aspire MC605 firmware version <= P11.A4L (latest) and Aspire TC-105 firmware version <= P12.B0L (latest) and Aspire TC-120 firmware version <= P11-A4	http://acer.com	O-ACE-VERI-121022/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(latest) and Aspire U5-620 firmware version <= P11.A1 (latest) and Aspire X1935 firmware version <= P11.A3L (latest) and Aspire X3475 firmware version <= P11.A3L (latest) and Aspire X3995 firmware version <= P11.A3L (latest) and Aspire XC100 firmware version <= P11.B3 (latest) and Aspire XC600 firmware version <= P11.A4 (latest) and Aspire Z3-615 firmware version <= P11.A2L (latest) and Veriton E430G firmware version <= P21.A1 (latest) and Veriton B630_49 firmware version <= AAP02SR (latest) and Veriton E430 firmware version <= P11.A4 (latest) and Veriton M2110G firmware version <= P21.A3 (latest) and Veriton M2120G fir. **CVE ID : CVE-2022-30426**		
Vendor: ami					
Product: aptio_v					
Affected Version(s): 5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Sep-2022	8.8	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for	https://www.ami.com/security-center/	O-AMI-APTI-121022/3834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hypervisors). This issue affects: Module name: SmmSmbiosElog SHA256: 3a8acb4f9bddccb19ec3b22b22ad97963711550f76b27b606461cd5073a93b59 Module GUID: 8e61fd6b-7a8b-404f-b83f-aa90a47cabdf This issue affects: AMI Aptio 5.x. This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-40250**		
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an	https://www.ami.com/security-center/	O-AMI-APTI-121022/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: PlatformInitAdvancedPreMem SHA256: 644044fdb8daea30a7820e0f5f88dbf5cd460af72fbf70418e9d2e47efed8d9b Module GUID: EEEE611D-F78F-4FB9-B868-55907F169280 This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-26873**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	8.2	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an	https://www.ami.com/security-center/	O-AMI-APTI-121022/3836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: OverClockSmiHandler SHA256: a204699576e1a48ce915d9d9423380c8e4c197003baf9d17e6504f0265f3039c Module GUID: 4698C2BD-A903-410E-AD1F-5EEF3A1AE422 **CVE ID : CVE-2022-40261**		
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and	https://www.ami.com/security-center/	O-AMI-APTI-121022/3837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: S3Resume2Pei SHA256: 7bb29f05534a8a1e010443213451425098faebd45948a4642db969b19d0253fc Module GUID: 89E549B0-7CFE-449D-9BA3-10D8B2312D71 **CVE ID : CVE-2022-40262**		
Out-of-bounds Write	20-Sep-2022	7.2	An attacker with physical access can exploit this vulnerability to execute arbitrary code during DXE phase. A malicious	https://www.ami.com/security-center/	O-AMI-APTI-121022/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code installed as a result of vulnerability exploitation in DXE driver could survive across an operating system (OS) boot process and runtime This issue affects: Module name: AMITSE SHA256: 288769fcb374d9280735e259c579e2dc209491f4da43b085d6aabc2d6e6ee57d Module GUID: b1da0adf-4f77-4070-a88e-bffe1c60529a This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-2154**		
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 15.4					
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193,	O-APP-IPAD-121022/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22629**	https://support.apple.com/en-us/HT213183	
Affected Version(s): * Up to (excluding) 15.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	9.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-32788**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3840
N/A	20-Sep-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-32802**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3841
Access of Resource Using Incompatible Type	23-Sep-2022	7.8	A type confusion issue was addressed with improved state handling. This issue is fixed in	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342,	O-APP-IPAD-121022/3842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32814**	https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Affected Version(s): * Up to (excluding) 15.7					
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32886**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3843
Out-of-bounds Read	20-Sep-2022	8.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32912		
Out-of-bounds Write	20-Sep-2022	7.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. A user may be able to elevate privileges. **CVE ID : CVE-2022-32908**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3845
N/A	20-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32911**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3846
Out-of-bounds Write	20-Sep-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An application may be	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support	O-APP-IPAD-121022/3847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-32917**	.apple.com/en-us/HT213446	
Incorrect Authorization	20-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32854**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3848
N/A	20-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32864**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3849
Exposure of Resource to Wrong Sphere	20-Sep-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-	O-APP-IPAD-121022/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32883**	us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
N/A	20-Sep-2022	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 16, iOS 15.7 and iPadOS 15.7. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2022-32795**	https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3851
N/A	20-Sep-2022	4.3	A logic issue was addressed with improved state management. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. A website may be able to track users through Safari web extensions. **CVE ID : CVE-2022-32868**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3852
N/A	20-Sep-2022	2.4	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16, iOS 15.7 and	https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPAD-121022/3853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7. A person with physical access to an iOS device may be able to access photos from the lock screen. **CVE ID : CVE-2022-32872**		
Product: ipad_os					
Affected Version(s): * Up to (excluding) 15.4					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-22610**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-121022/3854
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4, tvOS 15.4, Safari 15.4. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPAD-121022/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-22624**		
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22628**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-121022/3856
N/A	23-Sep-2022	8.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior. **CVE ID : CVE-2022-22637**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPAD-121022/3857
Affected Version(s): * Up to (excluding) 15.6					
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks.	https://support.apple.com/en-us/HT213344,	O-APP-IPAD-121022/3858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3859
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved input validation. This	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-	O-APP-IPAD-121022/3860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in iOS 15.6 and iPadOS 15.6, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32792**	us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213341, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3861
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://	O-APP-IPAD-121022/3862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32820**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3863
N/A	23-Sep-2022	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32821		
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3865
N/A	23-Sep-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32829**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3866
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8,	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-	O-APP-IPAD-121022/3867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	6.5	The issue was addressed with improved UI handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Visiting a website that frames malicious content may lead to UI spoofing. **CVE ID : CVE-2022-32816**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3868
NULL Pointer Dereference	23-Sep-2022	5.5	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing an	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image may lead to a denial-of-service. **CVE ID : CVE-2022-32785**		
Out-of-bounds Read	23-Sep-2022	5.5	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32817**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3870
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3871
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory	https://support.apple.com/en-us/HT213344,	O-APP-IPAD-121022/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32825**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32828**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3873
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2022-32841**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3875
N/A	23-Sep-2022	10	This issue was addressed with improved checks. This issue is fixed in watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to break out of its sandbox. **CVE ID : CVE-2022-32845**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPAD-121022/3876
Affected Version(s): * Up to (excluding) 15.5					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253,	O-APP-IPAD-121022/3877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.5, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-26700**	https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	O-APP-IPAD-121022/3878
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An app with root privileges may be able to access	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213258	O-APP-IPAD-121022/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			private information. **CVE ID : CVE-2022-32781**		
Product: iphone_os					
Affected Version(s): * Up to (excluding) 15.4					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-22610**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-121022/3880
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4, tvOS 15.4, Safari 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22624**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-IPHO-121022/3881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22628**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-121022/3882
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22629**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-IPHO-121022/3883
N/A	23-Sep-2022	8.8	A logic issue was addressed with improved state management. This issue is fixed in	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-	O-APP-IPHO-121022/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior. **CVE ID : CVE-2022-22637**	us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Affected Version(s): * Up to (excluding) 15.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	9.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-32788**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3885
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340,	O-APP-IPHO-121022/3886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3887
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213341, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32792		
N/A	20-Sep-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-32802**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3889
Access of Resource Using Incompatible Type ('Type Confusion')	23-Sep-2022	7.8	A type confusion issue was addressed with improved state handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32814**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3890
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342,	O-APP-IPHO-121022/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3892
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-	O-APP-IPHO-121022/3893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32820**	us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32821**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3894
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32829**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3896
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3897
N/A	23-Sep-2022	6.5	The issue was addressed with improved UI handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Visiting a	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support	O-APP-IPHO-121022/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			website that frames malicious content may lead to UI spoofing. **CVE ID : CVE-2022-32816**	.apple.com/en-us/HT213346	
NULL Pointer Dereference	23-Sep-2022	5.5	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2022-32785**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3899
Out-of-bounds Read	23-Sep-2022	5.5	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32817**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3900
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved	https://support.apple.com/en-us/HT213344, https://support	O-APP-IPHO-121022/3901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32825**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3902
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. An app may	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to disclose kernel memory. **CVE ID : CVE-2022-32828**		
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2022-32841**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3904
N/A	23-Sep-2022	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-IPHO-121022/3905
N/A	23-Sep-2022	10	This issue was addressed with improved checks.	https://support.apple.com/en-us/HT213345,	O-APP-IPHO-121022/3906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to break out of its sandbox. **CVE ID : CVE-2022-32845**	https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Affected Version(s): * Up to (excluding) 15.7					
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32886**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3907
Out-of-bounds Read	20-Sep-2022	8.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution.	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32912		
Out-of-bounds Write	20-Sep-2022	7.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. A user may be able to elevate privileges. **CVE ID : CVE-2022-32908**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3909
N/A	20-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32911**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3910
Out-of-bounds Write	20-Sep-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An application may be	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support	O-APP-IPHO-121022/3911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-32917**	.apple.com/en-us/HT213446	
Incorrect Authorization	20-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32854**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3912
N/A	20-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32864**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3913
N/A	20-Sep-2022	4.3	This issue was addressed with improved checks. This issue is fixed in iOS 16, iOS 15.7	https://support.apple.com/en-us/HT213445, https://support	O-APP-IPHO-121022/3914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 15.7. Visiting a malicious website may lead to address bar spoofing. **CVE ID : CVE-2022-32795**	.apple.com/en-us/HT213446	
N/A	20-Sep-2022	4.3	A logic issue was addressed with improved state management. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. A website may be able to track users through Safari web extensions. **CVE ID : CVE-2022-32868**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3915
N/A	20-Sep-2022	2.4	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16, iOS 15.7 and iPadOS 15.7. A person with physical access to an iOS device may be able to access photos from the lock screen. **CVE ID : CVE-2022-32872**	https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3916
Affected Version(s): * Up to (excluding) 15.5					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management.	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-	O-APP-IPHO-121022/3917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-26700**	us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	O-APP-IPHO-121022/3918
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213343, https://support	O-APP-IPHO-121022/3919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app with root privileges may be able to access private information. **CVE ID : CVE-2022-32781**	.apple.com/en-us/HT213258	
Affected Version(s): * Up to (excluding) 16.0					
Exposure of Resource to Wrong Sphere	20-Sep-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32883**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-IPHO-121022/3920
Product: macos					
Affected Version(s): -					
Use After Free	26-Sep-2022	8.8	Use after free in FedCM in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2852**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1349322	O-APP-MACO-121022/3921
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125	https://chromereleases.googleblog.com/2022/09/stable-	O-APP-MACO-121022/3922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3197**	channel-update-for-desktop_14.html, https://crbug.com/1358075	
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3196**	https://crbug.com/1358090, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html	O-APP-MACO-121022/3923
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3198**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1355682	O-APP-MACO-121022/3924
Use After Free	26-Sep-2022	8.8	Use after free in Frames in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1355237	O-APP-MACO-121022/3925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3199		
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Internals in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3200**	https://crbug.com/1355103, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html	O-APP-MACO-121022/3926
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28852**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3927
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28853**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38415**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3929
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38416**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38417**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38426**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3932
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38427**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38429**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3934
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38430**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38431**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3936
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38432**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.sue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38433**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3938
Use After Free	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38434**		
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35699**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3940
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35700**		
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35701**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3942
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35702**		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35703**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3944
Use After Free	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could result in	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35704**		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35705**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3946
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35706**		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35707**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3948
Heap-based	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3	https://helpx.adobe.com/security/products/br	O-APP-MACO-121022/3949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			(and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35708**	idge/apsb22-49.html	
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38405**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3950
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35713**		
N/A	20-Sep-2022	7.8	A vulnerability in the ClearPass OnGuard macOS agent could allow malicious users on a macOS instance to elevate their user privileges. A successful exploit could allow these users to execute arbitrary code with root level privileges on the macOS instance in Aruba ClearPass Policy Manager version(s): 6.10.x: 6.10.6 and below; 6.9.x: 6.9.11 and below. Aruba has released upgrades for Aruba ClearPass Policy Manager that address this security vulnerability. **CVE ID : CVE-2022-37877**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-013.txt	O-APP-MACO-121022/3952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38401**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3953
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38402**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38403**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3955
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38404**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Sep-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38408**	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	O-APP-MACO-121022/3957
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/animate/apsb22-54.html	O-APP-MACO-121022/3958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38411		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38412**	https://helpx.adobe.com/security/products/animate/apsb22-54.html	O-APP-MACO-121022/3959
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38413**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38414**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3961
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-28854**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28855**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3963
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28856**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28857**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3965
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30671**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30672**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3967
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30673**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30674**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3969
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30675**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30676**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-APP-MACO-121022/3971
Use After Free	16-Sep-2022	5.5	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-APP-MACO-121022/3972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38428**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38410**	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	O-APP-MACO-121022/3973
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38406**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38407**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-APP-MACO-121022/3975
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38425**		
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35709**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-APP-MACO-121022/3977
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory.	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	O-APP-MACO-121022/3978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38409**		
N/A	26-Sep-2022	4.3	Inappropriate implementation in Pointer Lock in Google Chrome on Mac prior to 105.0.5195.52 allowed a remote attacker to restrict user navigation via a crafted HTML page. **CVE ID : CVE-2022-3053**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1267867	O-APP-MACO-121022/3979
Affected Version(s): * Up to (excluding) 10.15.7					
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support	O-APP-MACO-121022/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or corrupt kernel memory. **CVE ID : CVE-2022-32847**	.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/3981
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support	O-APP-MACO-121022/3982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/3983
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32820**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/3984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/3985
Out-of-bounds Read	23-Sep-2022	7.8	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32842**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3986
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support	O-APP-MACO-121022/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	
N/A	23-Sep-2022	7.1	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32797**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3988
N/A	23-Sep-2022	7.1	This issue was addressed with improved file handling. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2022-32807**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32831**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3990
Out-of-bounds Write	23-Sep-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted Postscript file may result in unexpected app termination or disclosure of process memory. **CVE ID : CVE-2022-32843**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32851**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3992
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32853**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/3994
Out-of-bounds Read	23-Sep-2022	5.9	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. A user in a privileged network position may be able to leak sensitive information. **CVE ID : CVE-2022-32799**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3995
NULL Pointer Dereference	23-Sep-2022	5.5	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345,	O-APP-MACO-121022/3996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2022-32785**	https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32786**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3997
N/A	23-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parts of the file system. **CVE ID : CVE-2022-32800**		
N/A	23-Sep-2022	5.5	The issue was addressed with improved handling of caches. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32805**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/3999
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4000
N/A	23-Sep-2022	5.5	An information disclosure issue was addressed by	https://support.apple.com/en-us/HT213344,	O-APP-MACO-121022/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An app with root privileges may be able to access private information. **CVE ID : CVE-2022-32781**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213258	O-APP-MACO-121022/4002
Affected Version(s): 10.15.7					
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support	O-APP-MACO-121022/4003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4004
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342,	O-APP-MACO-121022/4005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4006
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-	O-APP-MACO-121022/4007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32820**	us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4008
Out-of-bounds Read	23-Sep-2022	7.8	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32842**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4009
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks.	https://support.apple.com/en-us/HT213256,	O-APP-MACO-121022/4010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	
N/A	23-Sep-2022	7.1	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32797**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4011
N/A	23-Sep-2022	7.1	This issue was addressed with improved file handling. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support	O-APP-MACO-121022/4012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.5. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2022-32807**	.apple.com/en-us/HT213343	
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32831**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4013
Out-of-bounds Write	23-Sep-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted Postscript file may result in unexpected app	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or disclosure of process memory. **CVE ID : CVE-2022-32843**		
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32851**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4015
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of process memory. **CVE ID : CVE-2022-32853**		
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4017
Out-of-bounds Read	23-Sep-2022	5.9	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. A user in a privileged network position may be able to leak sensitive information. **CVE ID : CVE-2022-32799**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	23-Sep-2022	5.5	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2022-32785**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4019
N/A	23-Sep-2022	5.5	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32786**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4020
N/A	23-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support	O-APP-MACO-121022/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32800**	.apple.com/en-us/HT213343	
N/A	23-Sep-2022	5.5	The issue was addressed with improved handling of caches. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32805**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4022
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32823		
N/A	23-Sep-2022	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4024
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An app with root privileges may be able to access private information. **CVE ID : CVE-2022-32781**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213258	O-APP-MACO-121022/4025
Affected Version(s): From (including) 11.0 Up to (excluding) 11.6.6					
N/A	20-Sep-2022	9.8	This issue was addressed with	https://support.apple.com/en-	O-APP-MACO-121022/4026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved checks. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32882**	us/HT213256, https://support.apple.com/en-us/HT213257	
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	O-APP-MACO-121022/4027
Affected Version(s): From (including) 11.0 Up to (excluding) 11.6.8					
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support	O-APP-MACO-121022/4028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4029
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340,	O-APP-MACO-121022/4030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4031
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32820		
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4033
N/A	23-Sep-2022	7.1	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32797**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4034
N/A	23-Sep-2022	7.1	This issue was addressed with	https://support.apple.com/en-	O-APP-MACO-121022/4035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved file handling. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2022-32807**	us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32831**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4036
Out-of-bounds Write	23-Sep-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support	O-APP-MACO-121022/4037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.6.8, macOS Monterey 12.5. Processing a maliciously crafted Postscript file may result in unexpected app termination or disclosure of process memory. **CVE ID : CVE-2022-32843**	.apple.com/en-us/HT213343	
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32851**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4038
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32853**		
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4040
NULL Pointer Dereference	23-Sep-2022	5.5	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343, https://support	O-APP-MACO-121022/4041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.5. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2022-32785**	.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32786**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4042
N/A	23-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32800**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4043
N/A	23-Sep-2022	5.5	The issue was addressed with improved handling	https://support.apple.com/en-us/HT213344,	O-APP-MACO-121022/4044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of caches. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32805**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4045
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-	O-APP-MACO-121022/4046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to disclose kernel memory. **CVE ID : CVE-2022-32825**	us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to capture a user's screen. **CVE ID : CVE-2022-32848**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4047
N/A	23-Sep-2022	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4048
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213257,	O-APP-MACO-121022/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An app with root privileges may be able to access private information. **CVE ID : CVE-2022-32781**	https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213258	
Affected Version(s): From (including) 11.0 Up to (excluding) 11.7					
Out-of-bounds Write	20-Sep-2022	7.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. A user may be able to elevate privileges. **CVE ID : CVE-2022-32908**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4050
N/A	20-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32911		
Out-of-bounds Write	20-Sep-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-32917**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4052
N/A	20-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32864**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4053
Exposure of Resource to Wrong Sphere	20-Sep-2022	5.5	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444,	O-APP-MACO-121022/4054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32883**	https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.7					
Incorrect Authorization	20-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32854**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4055
Affected Version(s): From (including) 12.0 Up to (excluding) 12.3					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution.	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-121022/4056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22610		
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4, tvOS 15.4, Safari 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22624**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213183	O-APP-MACO-121022/4057
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22628**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-MACO-121022/4058
N/A	23-Sep-2022	8.8	A logic issue was addressed with improved state management. This issue is fixed in	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-	O-APP-MACO-121022/4059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior. **CVE ID : CVE-2022-22637**	us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Affected Version(s): From (including) 12.0 Up to (excluding) 12.4					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-26700**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-MACO-121022/4060
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-	O-APP-MACO-121022/4061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	
N/A	23-Sep-2022	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4. An app may gain unauthorized access to Bluetooth. **CVE ID : CVE-2022-32783**	https://support.apple.com/en-us/HT213257	O-APP-MACO-121022/4062
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4, iOS 15.5 and iPadOS 15.5, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8. An app with root privileges may be able to access private information. **CVE ID : CVE-2022-32781**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213258	O-APP-MACO-121022/4063
N/A	23-Sep-2022	4.4	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.4. An	https://support.apple.com/en-us/HT213257	O-APP-MACO-121022/4064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app with root privileges may be able to access private information. **CVE ID : CVE-2022-32782**		
Affected Version(s): From (including) 12.0 Up to (excluding) 12.5					
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4065
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-	O-APP-MACO-121022/4066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32792**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213341, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4067
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support	O-APP-MACO-121022/4068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2022-32820**	.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4069
N/A	23-Sep-2022	7.8	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32829**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4070
N/A	23-Sep-2022	7.8	A memory corruption issue was addressed with improved state management.	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32796**		
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4072
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.5. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32798**	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4073
N/A	23-Sep-2022	7.8	A memory corruption issue was addressed	https://support.apple.com/en-us/HT213345,	O-APP-MACO-121022/4074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with improved validation. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32821**	https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.5. An app may be able to gain root privileges. **CVE ID : CVE-2022-32801**	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4075
Out-of-bounds Read	23-Sep-2022	7.8	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. An app may be able to gain elevated privileges. **CVE ID : CVE-2022-32842**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4076
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-	O-APP-MACO-121022/4077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	7.1	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted Postscript file may result in unexpected app termination or disclosure of process memory. **CVE ID : CVE-2022-32843**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4078
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support	O-APP-MACO-121022/4079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32851**	.apple.com/en-us/HT213343	
N/A	23-Sep-2022	7.1	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32797**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4080
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or disclosure of process memory. **CVE ID : CVE-2022-32852**		
N/A	23-Sep-2022	7.1	This issue was addressed with improved file handling. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2022-32807**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4082
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32853**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	23-Sep-2022	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing a maliciously crafted AppleScript binary may result in unexpected termination or disclosure of process memory. **CVE ID : CVE-2022-32831**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4084
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	6.5	The issue was addressed with improved UI handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Visiting a website that frames malicious content may lead to UI spoofing. **CVE ID : CVE-2022-32816**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4086
Out-of-bounds Read	23-Sep-2022	5.9	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in Security Update 2022-005 Catalina, macOS Monterey 12.5. A user in a privileged network position may be able to leak sensitive information. **CVE ID : CVE-2022-32799**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4087
N/A	23-Sep-2022	5.5	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in Security Update 2022-005 Catalina,	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32786**		
N/A	23-Sep-2022	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.5. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32789**	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4089
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32828**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4090
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.5. An app may be able to leak	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive kernel state. **CVE ID : CVE-2022-32818**		
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2022-32841**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4092
N/A	23-Sep-2022	5.5	The issue was addressed with improved handling of caches. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32805**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4093
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support	O-APP-MACO-121022/4094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	This issue was addressed with improved checks. This issue is fixed in Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to modify protected parts of the file system. **CVE ID : CVE-2022-32800**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343	O-APP-MACO-121022/4095
N/A	23-Sep-2022	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.8, macOS Monterey 12.5. An app may be able to capture a user's screen. **CVE ID : CVE-2022-32848**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4096
N/A	23-Sep-2022	5.5	An information disclosure issue	https://support.apple.com/en-	O-APP-MACO-121022/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32825**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4098
Out-of-bounds Read	23-Sep-2022	5.5	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support	O-APP-MACO-121022/4099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32817**	.apple.com/en-us/HT213346	
NULL Pointer Dereference	23-Sep-2022	5.5	A null pointer dereference was addressed with improved validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, Security Update 2022-005 Catalina, macOS Big Sur 11.6.8, macOS Monterey 12.5. Processing an image may lead to a denial-of-service. **CVE ID : CVE-2022-32785**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4100
N/A	23-Sep-2022	10	This issue was addressed with improved checks. This issue is fixed in watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to break out of its sandbox. **CVE ID : CVE-2022-32845**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4101
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.3					
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186,	O-APP-MACO-121022/4102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22629**	https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.4					
N/A	20-Sep-2022	9.8	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.4, macOS Big Sur 11.6.6. An app may be able to bypass Privacy preferences. **CVE ID : CVE-2022-32882**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257	O-APP-MACO-121022/4103
N/A	20-Sep-2022	8.8	This issue was addressed with improved environment sanitization. This issue is fixed in macOS Monterey 12.4. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2022-26696**	https://support.apple.com/en-us/HT213257	O-APP-MACO-121022/4104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	23-Sep-2022	5.5	An issue in the handling of environment variables was addressed with improved validation. This issue is fixed in macOS Monterey 12.4. A user may be able to view sensitive user information. **CVE ID : CVE-2022-26707**	https://support.apple.com/en-us/HT213257	O-APP-MACO-121022/4105
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.5					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	9.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-32788**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4106
Out-of-bounds Write	20-Sep-2022	9.8	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 15.6, macOS Monterey 12.5. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213341	O-APP-MACO-121022/4107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-32863**		
N/A	20-Sep-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-32802**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4108
Access of Resource Using Incompatible Type ('Type Confusion')	23-Sep-2022	7.8	A type confusion issue was addressed with improved state handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32814**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-MACO-121022/4109
N/A	20-Sep-2022	6.5	This issue was addressed by enabling hardened runtime. This issue is fixed in macOS Monterey 12.5. An app may be able to	https://support.apple.com/en-us/HT213345	O-APP-MACO-121022/4110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data. **CVE ID : CVE-2022-32880**		
N/A	20-Sep-2022	5.3	A logic issue was addressed with improved state management. This issue is fixed in Safari 15.6, macOS Monterey 12.5. A user may be tracked through their IP address. **CVE ID : CVE-2022-32861**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213341	O-APP-MACO-121022/4111
Affected Version(s): From (including) 12.0.0 Up to (excluding) 12.6					
Out-of-bounds Write	20-Sep-2022	7.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. A user may be able to elevate privileges. **CVE ID : CVE-2022-32908**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4112
N/A	20-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support	O-APP-MACO-121022/4113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32911**	.apple.com/en-us/HT213446	
Out-of-bounds Write	20-Sep-2022	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.. **CVE ID : CVE-2022-32917**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4114
N/A	20-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32864**	https://support.apple.com/en-us/HT213443, https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-APP-MACO-121022/4115
Exposure of Resource	20-Sep-2022	5.5	A logic issue was addressed with improved	https://support.apple.com/en-us/HT213443,	O-APP-MACO-121022/4116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			restrictions. This issue is fixed in macOS Monterey 12.6, iOS 15.7 and iPadOS 15.7, iOS 16, macOS Big Sur 11.7. An app may be able to read sensitive location information. **CVE ID : CVE-2022-32883**	https://support.apple.com/en-us/HT213444, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
Product: tvos					
Affected Version(s): * Up to (excluding) 15.4					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-22610**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-121022/4117
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support	O-APP-TVOS-121022/4118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22628**	.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22629**	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-TVOS-121022/4119
N/A	23-Sep-2022	8.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior.	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support	O-APP-TVOS-121022/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22637	.apple.com/en-us/HT213183	
Affected Version(s): * Up to (excluding) 15.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	9.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-32788**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4121
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4122
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds	https://support.apple.com/en-us/HT213344, https://support	O-APP-TVOS-121022/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32792**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213341, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4124
N/A	20-Sep-2022	7.8	A logic issue was addressed with improved checks. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6, macOS Monterey 12.5.	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support	O-APP-TVOS-121022/4125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted file may lead to arbitrary code execution. **CVE ID : CVE-2022-32802**	.apple.com/en-us/HT213346	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Sep-2022	7.8	A type confusion issue was addressed with improved state handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32814**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4126
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32815		
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4128
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32820**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4129
N/A	23-Sep-2022	7.8	A memory corruption issue	https://support.apple.com/en-	O-APP-TVOS-121022/4130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was addressed with improved validation. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32821**	us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4131
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support	O-APP-TVOS-121022/4132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	6.5	The issue was addressed with improved UI handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Visiting a website that frames malicious content may lead to UI spoofing. **CVE ID : CVE-2022-32816**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4133
Out-of-bounds Read	23-Sep-2022	5.5	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32817**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4135
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32825**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4136
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, tvOS 15.6,	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support	O-APP-TVOS-121022/4137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32828**	.apple.com/en-us/HT213346	
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2022-32841**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4138
N/A	23-Sep-2022	5.5	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to access sensitive user information. **CVE ID : CVE-2022-32849**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213346	O-APP-TVOS-121022/4139
Affected Version(s): * Up to (excluding) 15.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-26700**	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-TVOS-121022/4140
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	O-APP-TVOS-121022/4141
Product: watchos					
Affected Version(s): * Up to (excluding) 8.5					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed	https://support.apple.com/en-us/HT213186,	O-APP-WATC-121022/4142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2022-22610**	https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
Use After Free	23-Sep-2022	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22628**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-121022/4143
Out-of-bounds Write	23-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iTunes 12.12.3 for	https://support.apple.com/en-us/HT213188, https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support	O-APP-WATC-121022/4144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows, iOS 15.4 and iPadOS 15.4, tvOS 15.4. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-22629**	.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	
N/A	23-Sep-2022	8.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.3, Safari 15.4, watchOS 8.5, iOS 15.4 and iPadOS 15.4, tvOS 15.4. A malicious website may cause unexpected cross-origin behavior. **CVE ID : CVE-2022-22637**	https://support.apple.com/en-us/HT213186, https://support.apple.com/en-us/HT213187, https://support.apple.com/en-us/HT213182, https://support.apple.com/en-us/HT213193, https://support.apple.com/en-us/HT213183	O-APP-WATC-121022/4145
Affected Version(s): * Up to (excluding) 8.6					
N/A	23-Sep-2022	8.8	A memory corruption issue was addressed with improved state management. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, Safari 15.5. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213260, https://support.apple.com/en-us/HT213258	O-APP-WATC-121022/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to code execution. **CVE ID : CVE-2022-26700**		
N/A	23-Sep-2022	7.5	This issue was addressed with improved checks. This issue is fixed in tvOS 15.5, watchOS 8.6, iOS 15.5 and iPadOS 15.5, macOS Monterey 12.4, macOS Big Sur 11.6.6, Security Update 2022-004 Catalina. A remote user may be able to cause a denial-of-service. **CVE ID : CVE-2022-32790**	https://support.apple.com/en-us/HT213256, https://support.apple.com/en-us/HT213257, https://support.apple.com/en-us/HT213254, https://support.apple.com/en-us/HT213255, https://support.apple.com/en-us/HT213253, https://support.apple.com/en-us/HT213258	O-APP-WATC-121022/4147
Affected Version(s): * Up to (excluding) 8.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	9.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. A remote user may be able to cause kernel code execution. **CVE ID : CVE-2022-32788**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4148
N/A	23-Sep-2022	9.1	This issue was addressed with improved checks. This issue is fixed	https://support.apple.com/en-us/HT213344, https://support	O-APP-WATC-121022/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. A remote user may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2022-32847**	.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32787**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4150
Out-of-bounds Write	23-Sep-2022	8.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342,	O-APP-WATC-121022/4151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.6 and iPadOS 15.6, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32792**	https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213341, https://support.apple.com/en-us/HT213346	
Access of Resource Using Incompatible Type ('Type Confusion')	23-Sep-2022	7.8	A type confusion issue was addressed with improved state handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32814**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4152
N/A	23-Sep-2022	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340,	O-APP-WATC-121022/4153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32815**	https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32819**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4154
Out-of-bounds Write	23-Sep-2022	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges.	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32820		
N/A	23-Sep-2022	7.8	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32821**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4156
N/A	23-Sep-2022	7.8	An authorization issue was addressed with improved state management. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to gain root privileges. **CVE ID : CVE-2022-32826**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4157
N/A	23-Sep-2022	6.7	The issue was addressed with improved memory handling. This issue is fixed in iOS	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-	O-APP-WATC-121022/4158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app with root privileges may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2022-32832**	us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	6.5	The issue was addressed with improved UI handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Visiting a website that frames malicious content may lead to UI spoofing. **CVE ID : CVE-2022-32816**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4159
Out-of-bounds Read	23-Sep-2022	5.5	An out-of-bounds read issue was addressed with improved bounds checking. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support	O-APP-WATC-121022/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to disclose kernel memory. **CVE ID : CVE-2022-32817**	.apple.com/en-us/HT213346	
Improper Initialization	23-Sep-2022	5.5	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5, Security Update 2022-005 Catalina. An app may be able to leak sensitive user information. **CVE ID : CVE-2022-32823**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213343, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4161
N/A	23-Sep-2022	5.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Big Sur 11.6.8, watchOS 8.7, tvOS 15.6, macOS Monterey 12.5. An app may be able to disclose kernel memory. **CVE ID : CVE-2022-32825**	https://support.apple.com/en-us/HT213344, https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4162
N/A	23-Sep-2022	5.5	The issue was addressed with	https://support.apple.com/en-	O-APP-WATC-121022/4163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved memory handling. This issue is fixed in watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2022-32841**	us/HT213345, https://support.apple.com/en-us/HT213342, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	
N/A	23-Sep-2022	10	This issue was addressed with improved checks. This issue is fixed in watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to break out of its sandbox. **CVE ID : CVE-2022-32845**	https://support.apple.com/en-us/HT213345, https://support.apple.com/en-us/HT213340, https://support.apple.com/en-us/HT213346	O-APP-WATC-121022/4164
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-DEB-DEBI-121022/4165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-32886**		
Release of Invalid Pointer or Reference	19-Sep-2022	7.5	A denial-of-service issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. When many files exist, requesting Special:NewFiles with actor as a condition can result in a very long running query. **CVE ID : CVE-2022-28203**	https://phabricator.wikimedia.org/T297731	O-DEB-DEBI-121022/4166
Uncontrolled Recursion	19-Sep-2022	4.4	An issue was discovered in MediaWiki before 1.35.6, 1.36.x before 1.36.4, and 1.37.x before 1.37.2. Users with the editinterface permission can trigger infinite recursion, because a bare local interwiki is mishandled for the mainpage message. **CVE ID : CVE-2022-28201**	https://phabricator.wikimedia.org/T297571	O-DEB-DEBI-121022/4167
Affected Version(s): 11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32886**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-DEB-DEBI-121022/4168
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-DEB-DEBI-121022/4169
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-DEB-DEBI-121022/4170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			named crashes for lack of resources. **CVE ID : CVE-2022-38177**		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-DEB-DEBI-121022/4171
Vendor: Dell					
Product: smartfabric_os10					
Affected Version(s): 10.5.3.4					
Improper Certificate Validation	28-Sep-2022	3.7	Dell OS10, version 10.5.3.4, contains an Improper Certificate Validation vulnerability in Support Assist. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to unauthorized access to limited switch configuration data. The vulnerability could be leveraged	https://www.dell.com/support/kbdoc/en-us/000202974/dsa-2022-293-dell-networking-os10-security-update-for-a-support-assist-vulnerability	O-DEL-SMAR-121022/4172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by attackers to conduct man-in-the-middle attacks to gain access to the Support Assist information. **CVE ID : CVE-2022-34394**		
Affected Version(s): From (including) 10.5.1.0 Up to (excluding) 10.5.1.11					
Out-of-bounds Write	28-Sep-2022	7.5	Networking OS10, versions 10.5.1.x, 10.5.2.x, and 10.5.3.x contain a vulnerability that could allow an attacker to cause a system crash by running particular security scans. **CVE ID : CVE-2022-34424**	https://www.dell.com/support/kbdoc/en-us/000202971/dsa-2022-135-dell-emc-smartfabric-os10-security-update-for-multiple-security-vulnerabilities	O-DEL-SMAR-121022/4173
Insufficiently Protected Credentials	28-Sep-2022	4.9	Dell Networking OS10, versions prior to October 2021 with Smart Fabric Services enabled, contains an information disclosure vulnerability. A remote, unauthenticated attacker could potentially exploit this vulnerability by reverse engineering to retrieve sensitive information and access the REST API with admin privileges.	https://www.dell.com/support/kbdoc/en-us/000202971/dsa-2022-135-dell-emc-smartfabric-os10-security-update-for-multiple-security-vulnerabilities	O-DEL-SMAR-121022/4174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29089		
Affected Version(s): From (including) 10.5.2.0 Up to (excluding) 10.5.2.11					
Out-of-bounds Write	28-Sep-2022	7.5	Networking OS10, versions 10.5.1.x, 10.5.2.x, and 10.5.3.x contain a vulnerability that could allow an attacker to cause a system crash by running particular security scans. **CVE ID : CVE-2022-34424**	https://www.dell.com/support/kbdoc/en-us/000202971/dsa-2022-135-dell-emc-smartfabric-os10-security-update-for-multiple-security-vulnerabilities	O-DEL-SMAR-121022/4175
Insufficiently Protected Credentials	28-Sep-2022	4.9	Dell Networking OS10, versions prior to October 2021 with Smart Fabric Services enabled, contains an information disclosure vulnerability. A remote, unauthenticated attacker could potentially exploit this vulnerability by reverse engineering to retrieve sensitive information and access the REST API with admin privileges. **CVE ID : CVE-2022-29089**	https://www.dell.com/support/kbdoc/en-us/000202971/dsa-2022-135-dell-emc-smartfabric-os10-security-update-for-multiple-security-vulnerabilities	O-DEL-SMAR-121022/4176
Affected Version(s): From (including) 10.5.3.0 Up to (excluding) 10.5.3.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	28-Sep-2022	7.5	Networking OS10, versions 10.5.1.x, 10.5.2.x, and 10.5.3.x contain a vulnerability that could allow an attacker to cause a system crash by running particular security scans. **CVE ID : CVE-2022-34424**	https://www.dell.com/support/kbdoc/en-us/000202971/dsa-2022-135-dell-emc-smartfabric-os10-security-update-for-multiple-security-vulnerabilities	O-DEL-SMAR-121022/4177
Insufficiently Protected Credentials	28-Sep-2022	4.9	Dell Networking OS10, versions prior to October 2021 with Smart Fabric Services enabled, contains an information disclosure vulnerability. A remote, unauthenticated attacker could potentially exploit this vulnerability by reverse engineering to retrieve sensitive information and access the REST API with admin privileges. **CVE ID : CVE-2022-29089**	https://www.dell.com/support/kbdoc/en-us/000202971/dsa-2022-135-dell-emc-smartfabric-os10-security-update-for-multiple-security-vulnerabilities	O-DEL-SMAR-121022/4178
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 35					
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory	https://support.apple.com/en-us/HT213442, https://support	O-FED-FEDO-121022/4179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32886**	.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.com/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6903b9e41fe7cb70030e8750	O-FED-FEDO-121022/4180
Affected Version(s): 36					
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-FED-FEDO-121022/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2022-32886**		
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4182
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4183
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38177**		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4185
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.com/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6903b9e41fe7cb70030e8750	O-FED-FEDO-121022/4186
Affected Version(s): 37					
Integer Overflow	23-Sep-2022	9.8	Redis is an in-memory database	https://github.com/redis/redis	O-FED-FEDO-121022/4187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			that persists on disk. Versions 7.0.0 and above, prior to 7.0.5 are vulnerable to an Integer Overflow. Executing an `XAUTOCLAIM` command on a stream key in a specific state, with a specially crafted `COUNT` argument may cause an integer overflow, a subsequent heap overflow, and potentially lead to remote code execution. This has been patched in Redis version 7.0.5. No known workarounds exist. **CVE ID : CVE-2022-35951**	/security/advisories/GHSA-5gc4-76rx-22c9	
Out-of-bounds Write	20-Sep-2022	8.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in Safari 16, iOS 16, iOS 15.7 and iPadOS 15.7. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2022-32886**	https://support.apple.com/en-us/HT213442, https://support.apple.com/en-us/HT213445, https://support.apple.com/en-us/HT213446	O-FED-FEDO-121022/4188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	21-Sep-2022	7.5	By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. **CVE ID : CVE-2022-2795**	https://kb.isc.org/docs/cve-2022-2795, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4189
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Sep-2022	7.5	By sending specific queries to the resolver, an attacker can cause named to crash. **CVE ID : CVE-2022-3080**	https://kb.isc.org/docs/cve-2022-3080, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4190
Uncontrolled Resource Consumption	26-Sep-2022	7.5	A vulnerability named 'Non-Responsive Delegation Attack' (NRDelegation Attack) has been discovered in various DNS resolving software. The NRDelegation Attack works by having a malicious delegation with a considerable number of non responsive	https://www.nlnetlabs.nl/downloads/unbound/CVE-2022-3204.txt	O-FED-FEDO-121022/4191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nameservers. The attack starts by querying a resolver for a record that relies on those unresponsive nameservers. The attack can cause a resolver to spend a lot of time/resources resolving records under a malicious delegation point where a considerable number of unresponsive NS records reside. It can trigger high CPU usage in some resolver implementations that continually look in the cache for resolved NS records in that delegation. This can lead to degraded performance and eventually denial of service in orchestrated attacks. Unbound does not suffer from high CPU usage, but resources are still needed for resolving the malicious delegation. Unbound will keep		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trying to resolve the record until hard limits are reached. Based on the nature of the attack and the replies, different limits could be reached. From version 1.16.3 on, Unbound introduces fixes for better performance when under load, by cutting opportunistic queries for nameserver discovery and DNSKEY prefetching and limiting the number of times a delegation point can issue a cache lookup for missing records. **CVE ID : CVE-2022-3204**		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.	https://kb.isc.org/docs/cve-2022-38177, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38177		
Improper Verification of Cryptographic Signature	21-Sep-2022	7.5	By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE ID : CVE-2022-38178**	https://kb.isc.org/docs/cve-2022-38178, http://www.openwall.com/lists/oss-security/2022/09/21/3	O-FED-FEDO-121022/4193
Uncontrolled Resource Consumption	23-Sep-2022	7.5	Knot Resolver before 5.5.3 allows remote attackers to cause a denial of service (CPU consumption) because of algorithmic complexity. During an attack, an authoritative server must return large NS sets or address sets. **CVE ID : CVE-2022-40188**	https://gitlab.nic.cz/knot/knot-resolver/-/merge_requests/1343#note_262558	O-FED-FEDO-121022/4194
Authentication Bypass by Spoofing	20-Sep-2022	6.6	Grafana is an open-source platform for monitoring and observability. Versions prior to 9.1.6 and 8.5.13 are vulnerable to an escalation from	https://github.com/grafana/grafana/security/advisories/GHSA-ff5c-938w-8c9q	O-FED-FEDO-121022/4195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin to server admin when auth proxy is used, allowing an admin to take over the server admin account and gain full control of the grafana instance. All installations should be upgraded as soon as possible. As a workaround deactivate auth proxy following the instructions at: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/configure-authentication/auth-proxy/ **CVE ID : CVE-2022-35957**		
Out-of-bounds Write	19-Sep-2022	5.5	A heap buffer overflow issue was found in ImageMagick. When an application processes a malformed TIFF file, it could lead to undefined behavior or a crash causing a denial of service. **CVE ID : CVE-2022-3213**	https://bugzilla.redhat.com/show_bug.cgi?id=2126824, https://github.com/ImageMagick/ImageMagick/commit/30ccf9a0da1f47161b5935a95be854fe84e6c2a2, https://github.com/ImageMagick/ImageMagick6/commit/1aea203eb36409ce6	O-FED-FEDO-121022/4196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				903b9e41fe7cb70030e8750	
Vendor: Festo					
Product: cpx-cec-c1_firmware					
Affected Version(s): * Up to (including) 1.2.34					
Improper Privilege Management	20-Sep-2022	7.5	Festo control block CPX-CEC-C1 and CPX-CMXX in multiple versions allow unauthenticated, remote access to critical webpage functions which may cause a denial of service. **CVE ID : CVE-2022-3079**	https://cert.vde.com/en/advisories/VDE-2022-036	O-FES-CPX--121022/4197
Product: cpx-cmxx_firmware					
Affected Version(s): * Up to (including) 2.0.12					
Improper Privilege Management	20-Sep-2022	7.5	Festo control block CPX-CEC-C1 and CPX-CMXX in multiple versions allow unauthenticated, remote access to critical webpage functions which may cause a denial of service. **CVE ID : CVE-2022-3079**	https://cert.vde.com/en/advisories/VDE-2022-036	O-FES-CPX--121022/4198
Vendor: gavazziautomation					
Product: uwp_3.0_monitoring_gateway_and_controller_firmware					
Affected Version(s): * Up to (excluding) 8.5.0.3					
Use of Hard-	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY	https://cert.vde.com/en/adviso	O-GAV-UWP_-121022/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials to gain full access to the device. **CVE ID : CVE-2022-22522**	ries/VDE-2022-029/	
Missing Authentication for Critical Function	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a missing authentication allows for full access via API. **CVE ID : CVE-2022-22526**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4200
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could utilize an improper input validation on an API-submitted parameter to execute arbitrary OS commands. **CVE ID : CVE-2022-28811**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4201
Use of Hard-coded Credentials	28-Sep-2022	9.8	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version 2.8.3 a remote, unauthenticated attacker could make use of hard-coded credentials to gain SuperUser access to the device. **CVE ID : CVE-2022-28812**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	9.8	Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 was discovered to be vulnerable to a relative path traversal vulnerability which enables remote attackers to read arbitrary files and gain full control of the device. **CVE ID : CVE-2022-28814**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4203
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	9.4	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 an unauthenticated remote attacker could utilize a SQL-Injection vulnerability to gain full database access, modify users and stop services .	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22524		
Improper Authentication	28-Sep-2022	7.5	An improper authentication vulnerability exists in the Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 Web-App which allows an authentication bypass to the context of an unauthorised user if free-access is disabled. **CVE ID : CVE-2022-22523**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4205
Improper Input Validation	28-Sep-2022	7.2	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 an remote attacker with admin rights could execute arbitrary commands due to missing input sanitization in the backup restore function **CVE ID : CVE-2022-22525**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4206
Improper Neutralization of Input During Web Page	28-Sep-2022	6.1	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 the Sentilo Proxy is	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			prone to reflected XSS which only affects the Sentilo service. **CVE ID : CVE-2022-28816**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	5.3	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 a remote, unauthenticated attacker could make use of an SQL-injection to gain access to a volatile temporary database with the current states of the device. **CVE ID : CVE-2022-28813**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4208
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Sep-2022	2.7	In Carlo Gavazzi UWP3.0 in multiple versions and CPY Car Park Server in Version 2.8.3 the Sentilo Proxy server was discovered to contain a SQL injection vulnerability allowing an attacker to query other tables of the Sentilo service. **CVE ID : CVE-2022-28815**	https://cert.vde.com/en/advisories/VDE-2022-029/	O-GAV-UWP_-121022/4209
Vendor: Google					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: android					
Affected Version(s): -					
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Downloads in Google Chrome on Android prior to 104.0.5112.101 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2853**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1350097	O-GOO-ANDR-121022/4210
Improper Input Validation	26-Sep-2022	6.5	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 104.0.5112.101 allowed a remote attacker to arbitrarily browse to a malicious website via a crafted HTML page. **CVE ID : CVE-2022-2856**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1345630	O-GOO-ANDR-121022/4211
Product: chrome_os					
Affected Version(s): -					
Use After Free	26-Sep-2022	8.8	Use after free in PhoneHub in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-	O-GOO-CHRO-121022/4212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3042**	desktop_30.html, https://crbug.com/1338553	
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Screen Capture in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3043**	https://crbug.com/1336979, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	O-GOO-CHRO-121022/4213
Use After Free	26-Sep-2022	8.8	Use after free in SplitScreen in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3049**	https://crbug.com/1316892, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	O-GOO-CHRO-121022/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in WebUI in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3050**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1337132	O-GOO-CHRO-121022/4215
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Exosphere in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3051**	https://crbug.com/1345245, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	O-GOO-CHRO-121022/4216
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Window Manager in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html,	O-GOO-CHRO-121022/4217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. **CVE ID : CVE-2022-3052**	https://crbug.com/1346154	
Use After Free	26-Sep-2022	8.8	Use after free in Tab Strip in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interaction. **CVE ID : CVE-2022-3071**	https://crbug.com/1333995, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	O-GOO-CHRO-121022/4218
Missing Authorization	26-Sep-2022	6.8	Inappropriate implementation in Chrome OS lockscreen in Google Chrome on Chrome OS prior to 105.0.5195.52 allowed a local attacker to bypass lockscreen navigation restrictions via physical access to the device. **CVE ID : CVE-2022-3048**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html, https://crbug.com/1303308	O-GOO-CHRO-121022/4219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	26-Sep-2022	5.4	Insufficient validation of untrusted input in DevTools in Google Chrome on Chrome OS prior to 105.0.5195.125 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2022-3201**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1343104	O-GOO-CHRO-121022/4220
Product: linux_and_chrome_os					
Affected Version(s): -					
Use After Free	26-Sep-2022	8.8	Use after free in SplitScreen in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3049**	https://crbug.com/1316892, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html	O-GOO-LINU-121022/4221
Use After Free	26-Sep-2022	8.8	Use after free in Tab Strip in Google Chrome on Chrome OS, Lacros prior to 105.0.5195.52 allowed a remote	https://crbug.com/1333995, https://chromereleases.googleblog.com/2022/08/stable-	O-GOO-LINU-121022/4222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interaction. **CVE ID : CVE-2022-3071**	channel-update-for-desktop_30.html	
Vendor: Grandstream					
Product: gds3710_firmware					
Affected Version(s): 1.0.11.13					
Out-of-bounds Write	23-Sep-2022	9.8	an attacker with knowledge of user/pass of Grandstream GSD3710 in its 1.0.11.13 version, could overflow the stack since it doesn't check the param length before use the strcopy instruction. The explotation of this vulnerability may lead an attacker to execute a shell with full access. **CVE ID : CVE-2022-2025**	https://www.incibe-cert.es/en/early-warning/security-advisories/buffer-overflow-vulnerabilities-grandstream-gsd3710	O-GRA-GDS3-121022/4223
Out-of-bounds Write	23-Sep-2022	9.8	In Grandstream GSD3710 in its 1.0.11.13 version, it's possible to overflow the stack since it doesn't check the param length before using the sscanf	https://www.incibe-cert.es/en/early-warning/security-advisories/buffer-overflow-vulnerabilities-	O-GRA-GDS3-121022/4224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instruction. Because of that, an attacker could create a socket and connect with a remote IP:port by opening a shell and getting full access to the system. The exploit affects daemons dbmng and logsrv that are running on ports 8000 and 8001 by default. **CVE ID : CVE-2022-2070**	grandstream-gsd3710	
Vendor: hpe					
Product: integrated_lights-out_5_firmware					
Affected Version(s): * Up to (excluding) 2.72					
N/A	20-Sep-2022	8.8	A remote potential adjacent denial of service (DoS) and potential adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	O-HPE-INTE-121022/4225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses these security vulnerabilities. **CVE ID : CVE-2022-28639**		
N/A	20-Sep-2022	8.8	A potential local adjacent arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability was discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses this security vulnerability. **CVE ID : CVE-2022-28640**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	O-HPE-INTE-121022/4226
N/A	20-Sep-2022	7.8	A local Denial of Service (DoS) and local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71.	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	O-HPE-INTE-121022/4227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28637**		
N/A	20-Sep-2022	7.8	An isolated local disclosure of information and potential isolated local arbitrary code execution vulnerability that could potentially lead to a loss of confidentiality, integrity, and availability were discovered in HPE Integrated Lights-Out 5 (iLO 5) in Version: 2.71. Hewlett Packard Enterprise has provided updated firmware for HPE Integrated Lights-Out 5 (iLO 5) that addresses these security vulnerabilities. **CVE ID : CVE-2022-28638**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf04365en_us	O-HPE-INTE-121022/4228
Vendor: Huawei					
Product: cv81-wdm_fw_firmware					
Affected Version(s): 01.70.49.29.46					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	20-Sep-2022	7.5	A Huawei device has an input verification vulnerability. Successful exploitation of this vulnerability may lead to DoS attacks.Affected product versions include:CV81-WDM FW versions 01.70.49.29.46. **CVE ID : CVE-2022-37395**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220810-01-8cfecdcc-en	O-HUA-CV81-121022/4229
Product: emui					
Affected Version(s): 10.1.0					
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38978**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4230
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/	O-HUA-EMUI-121022/4231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38987**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4232
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38988**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4233
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38989**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38990**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4235
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38991**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4236
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38992**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4237
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful	https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-EMUI-121022/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	ity-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4239
Affected Version(s): 10.1.1					
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38978**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4240
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-	O-HUA-EMUI-121022/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect data confidentiality. **CVE ID : CVE-2022-38979**	000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38987**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4242
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38988**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4243
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38989**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/	O-HUA-EMUI-121022/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38990**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4245
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38991**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4246
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38992**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4248
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4249
Affected Version(s): 11.0.0					
N/A	16-Sep-2022	9.8	The iAware module has a vulnerability in managing malicious apps.Successful exploitation of this vulnerability will cause malicious apps to automatically start upon system startup. **CVE ID : CVE-2022-39000**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	16-Sep-2022	9.8	Double free vulnerability in the storage module. Successful exploitation of this vulnerability will cause the memory to be freed twice. **CVE ID : CVE-2022-39002**	https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4251
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.1	Buffer overflow vulnerability in the video framework. Successful exploitation of this vulnerability will affect the confidentiality and integrity of trusted components. **CVE ID : CVE-2022-39003**	https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4252
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38978**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4253
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-	O-HUA-EMUI-121022/4254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect data confidentiality. **CVE ID : CVE-2022-38979**	000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4255
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	7.5	The number identification module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause data disclosure. **CVE ID : CVE-2022-39001**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4256
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/	O-HUA-EMUI-121022/4257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39004	en/support/bulletin/2022/9/	
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4258
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Sep-2022	5.9	The MPTCP module has the race condition vulnerability. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2022-39006**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4259
Affected Version(s): 11.0.1					
N/A	16-Sep-2022	9.8	The iAware module has a vulnerability in managing malicious apps.Successful exploitation of this vulnerability will cause malicious apps to automatically start upon system startup.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39000		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	7.5	The number identification module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause data disclosure. **CVE ID : CVE-2022-39001**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4261
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4262
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Sep-2022	5.9	The MPTCP module has the race condition vulnerability. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2022-39006**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4264
Affected Version(s): 12.0.0					
N/A	16-Sep-2022	9.8	The AOD module has the improper update of reference count vulnerability. Successful exploitation of this vulnerability may affect data integrity, confidentiality, and availability. **CVE ID : CVE-2022-38999**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4265
N/A	16-Sep-2022	9.8	The iAware module has a vulnerability in managing malicious apps.Successful exploitation of this vulnerability will cause malicious apps to automatically start upon system startup. **CVE ID : CVE-2022-39000**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	9.8	The location module has a vulnerability of bypassing permission verification.Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-39007**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4267
Improper Authentication	16-Sep-2022	9.8	The WLAN module has a vulnerability in permission verification. Successful exploitation of this vulnerability may cause third-party apps to affect WLAN functions. **CVE ID : CVE-2022-39009**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4268
Deserialization of Untrusted Data	16-Sep-2022	9.1	The NFC module has bundle serialization/deserialization vulnerabilities. Successful exploitation of this vulnerability may cause third-party apps to read and write files that are accessible only to system apps. **CVE ID : CVE-2022-39008**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38978**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4270
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4271
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38987**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4272
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful	https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-EMUI-121022/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38988**	ity-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38989**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4274
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38990**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4275
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227	O-HUA-EMUI-121022/4276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38991	8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38992**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4277
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4278
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38994**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/	O-HUA-EMUI-121022/4279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38995**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4280
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38996**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4281
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	7.5	The number identification module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause data disclosure. **CVE ID : CVE-2022-39001**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4283
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4284
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4285
N/A	16-Sep-2022	7.5	The HwChrService module has a vulnerability in permission control.	https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-EMUI-121022/4286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may cause disclosure of user network information. **CVE ID : CVE-2022-39010**	ity-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Sep-2022	5.9	The MPTCP module has the race condition vulnerability. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2022-39006**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-EMUI-121022/4287
Product: harmonyos					
Affected Version(s): 2.0					
N/A	16-Sep-2022	9.8	The AOD module has the improper update of reference count vulnerability. Successful exploitation of this vulnerability may affect data integrity, confidentiality, and availability. **CVE ID : CVE-2022-38999**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4288
N/A	16-Sep-2022	9.8	The iAware module has a vulnerability in managing malicious apps.Successful	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-HARM-121022/4289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability will cause malicious apps to automatically start upon system startup. **CVE ID : CVE-2022-39000**	phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
Improper Authentication	16-Sep-2022	9.8	The location module has a vulnerability of bypassing permission verification.Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-39007**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4290
Improper Authentication	16-Sep-2022	9.8	The WLAN module has a vulnerability in permission verification. Successful exploitation of this vulnerability may cause third-party apps to affect WLAN functions. **CVE ID : CVE-2022-39009**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4291
Deserialization of Untrusted Data	16-Sep-2022	9.1	The NFC module has bundle serialization/deserialization vulnerabilities. Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-	O-HUA-HARM-121022/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause third-party apps to read and write files that are accessible only to system apps. **CVE ID : CVE-2022-39008**	000000139227 8845, https://consum er.huawei.com/ en/support/bul letin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38978**	https://device.h armonyos.com/ en/docs/securit y/update/secur ity-bulletins-phones-202209-000000139227 8845, https://consum er.huawei.com/ en/support/bul letin/2022/9/	O-HUA-HARM-121022/4293
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.h armonyos.com/ en/docs/securit y/update/secur ity-bulletins-phones-202209-000000139227 8845, https://consum er.huawei.com/ en/support/bul letin/2022/9/	O-HUA-HARM-121022/4294
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability.	https://device.h armonyos.com/ en/docs/securit y/update/secur ity-bulletins-phones-202209-000000139227 8845,	O-HUA-HARM-121022/4295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38987	https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38988**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4296
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38989**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4297
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38990**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38991**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4299
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38992**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4300
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4301
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful	https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-HARM-121022/4302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38994**	ity-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38995**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4303
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38996**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4304
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227	O-HUA-HARM-121022/4305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38997	8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	7.5	The number identification module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause data disclosure. **CVE ID : CVE-2022-39001**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4306
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4307
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/	O-HUA-HARM-121022/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The HwChrService module has a vulnerability in permission control. Successful exploitation of this vulnerability may cause disclosure of user network information. **CVE ID : CVE-2022-39010**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4309
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Sep-2022	5.9	The MPTCP module has the race condition vulnerability. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2022-39006**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4310
Affected Version(s): 2.1					
N/A	16-Sep-2022	9.8	The iAware module has a vulnerability in managing malicious apps.Successful exploitation of this vulnerability will cause malicious apps to automatically start upon system startup.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39000		
Improper Authentication	16-Sep-2022	9.8	The location module has a vulnerability of bypassing permission verification.Successful exploitation of this vulnerability may cause privilege escalation. **CVE ID : CVE-2022-39007**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4312
Improper Authentication	16-Sep-2022	9.8	The WLAN module has a vulnerability in permission verification. Successful exploitation of this vulnerability may cause third-party apps to affect WLAN functions. **CVE ID : CVE-2022-39009**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4313
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38978**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4315
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4316
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38994**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4317
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful	https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-HARM-121022/4318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38995**	ity-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38996**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4319
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4320
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227	O-HUA-HARM-121022/4321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause memory leaks. **CVE ID : CVE-2022-39004**	8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4322
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Sep-2022	5.9	The MPTCP module has the race condition vulnerability. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2022-39006**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-HARM-121022/4323
Product: magic_ui					
Affected Version(s): 3.1.0					
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845,	O-HUA-MAGI-121022/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38978	https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4325
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38987**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4326
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38988**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38989**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4328
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38990**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4329
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38991**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4330
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful	https://device.harmonyos.com/en/docs/security/update/secur	O-HUA-MAGI-121022/4331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38992**	ity-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4332
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4333
Affected Version(s): 3.1.1					
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-	O-HUA-MAGI-121022/4334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect data confidentiality. **CVE ID : CVE-2022-38978**	000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4335
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38987**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4336
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38988**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/	O-HUA-MAGI-121022/4337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38989**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4338
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38990**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4339
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38991**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38992**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4341
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-38993**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4342
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4343
Affected Version(s): 4.0.0					
N/A	16-Sep-2022	9.8	The iAware module has a vulnerability in managing	https://device.harmonyos.com/en/docs/securit	O-HUA-MAGI-121022/4344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious apps.Successful exploitation of this vulnerability will cause malicious apps to automatically start upon system startup. **CVE ID : CVE-2022-39000**	y/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	
Double Free	16-Sep-2022	9.8	Double free vulnerability in the storage module. Successful exploitation of this vulnerability will cause the memory to be freed twice. **CVE ID : CVE-2022-39002**	https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4345
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.1	Buffer overflow vulnerability in the video framework. Successful exploitation of this vulnerability will affect the confidentiality and integrity of trusted components. **CVE ID : CVE-2022-39003**	https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4346
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845,	O-HUA-MAGI-121022/4347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38978	https://consumer.huawei.com/en/support/bulletin/2022/9/	
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38979**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4348
N/A	16-Sep-2022	7.5	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-38997**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4349
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Sep-2022	7.5	The number identification module has a path traversal vulnerability. Successful exploitation of this vulnerability may cause data disclosure. **CVE ID : CVE-2022-39001**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-0000001392278845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4351
Missing Release of Memory after Effective Lifetime	16-Sep-2022	7.5	The MPTCP module has the memory leak vulnerability. Successful exploitation of this vulnerability can cause memory leaks. **CVE ID : CVE-2022-39005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4352
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Sep-2022	5.9	The MPTCP module has the race condition vulnerability. Successful exploitation of this vulnerability may cause the device to restart. **CVE ID : CVE-2022-39006**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202209-000000139227 8845, https://consumer.huawei.com/en/support/bulletin/2022/9/	O-HUA-MAGI-121022/4353
Product: ws7200-10_firmware					
Affected Version(s): 11.0.2.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	20-Sep-2022	6.5	There is a password verification vulnerability in WS7200-10 11.0.2.13. Attackers on the LAN may use brute force cracking to obtain passwords, which may cause sensitive system information to be disclosed. **CVE ID : CVE-2022-33735**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220628-01-2eda0853-en	O-HUA-WS72-121022/4354
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Input Validation	23-Sep-2022	5.5	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596. **CVE ID : CVE-2022-22423**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223596, https://www.ibm.com/support/pages/node/6695893	O-IBM-AIX-121022/4355
Improper Neutralization of Input During Web Page Generation	23-Sep-2022	5.4	IBM Jazz for Service Management 1.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary	https://www.ibm.com/support/pages/node/6695811, https://exchange.xforce.ibmcloud.com/vulnerabilities/231380	O-IBM-AIX-121022/4356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 231380. **CVE ID : CVE-2022-35721**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236586. **CVE ID : CVE-2022-40748**	https://exchange.xforce.ibmcloud.com/vulnerabilities/236586, https://www.ibm.com/support/pages/node/6695961	O-IBM-AIX-121022/4357
Product: i					
Affected Version(s): -					
Improper Input Validation	23-Sep-2022	5.5	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could	https://exchange.xforce.ibmcloud.com/vulnerabilities/223596, https://www.ibm.com/support	O-IBM-I-121022/4358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596. **CVE ID : CVE-2022-22423**	/pages/node/6695893	
Product: powerlinux					
Affected Version(s): -					
Improper Input Validation	23-Sep-2022	5.5	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596. **CVE ID : CVE-2022-22423**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223596, https://www.ibm.com/support/pages/node/6695893	O-IBM-POWE-121022/4359
Vendor: iegeek					
Product: ig20_firmware					
Affected Version(s): -					
Use of Insufficiently Random Values	26-Sep-2022	6.5	ieGeek IG20 hipcam RealServer V1.0 is vulnerable to Incorrect Access Control. The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw	N/A	O-IEG-IG20-121022/4360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that allows remote attackers to establish direct connections to arbitrary devices. **CVE ID : CVE-2022-38970**		
Vendor: Intel					
Product: nuc_m15_laptop_kit_lapbc510_firmware					
Affected Version(s): -					
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: PlatformInitAdvancedPreMem	https://www.ami.com/security-center/	O-INT-NUC_-121022/4361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SHA256: 644044fdb8daea30a7820e0f5f88dbf5cd460af72fbf70418e9d2e47efed8d9b Module GUID: EEEE611D-F78F-4FB9-B868-55907F169280 This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-26873**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	8.2	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system	https://www.ami.com/security-center/	O-INT-NUC_-121022/4362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: OverClockSmiHandler SHA256: a204699576e1a48ce915d9d9423380c8e4c197003baf9d17e6504f0265f3039c Module GUID: 4698C2BD-A903-410E-AD1F-5EEF3A1AE422 **CVE ID : CVE-2022-40261**		
Affected Version(s): 0072					
Out-of-bounds Write	20-Sep-2022	7.2	An attacker with physical access can exploit this vulnerability to execute arbitrary code during DXE phase. A malicious code installed as a result of vulnerability exploitation in DXE driver could survive across an	https://www.ami.com/security-center/	O-INT-NUC_-121022/4363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system (OS) boot process and runtime This issue affects: Module name: AMITSE SHA256: 288769fcb374d9280735e259c579e2dc209491f4da43b085d6aabc2d6e6ee57d Module GUID: b1da0adf-4f77-4070-a88e-bffe1c60529a This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-2154**		
Out-of-bounds Write	20-Sep-2022	7.2	A potential attacker can write one byte by arbitrary address at the time of the PEI phase (only during S3 resume boot mode) and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries.	https://www.ami.com/security-center/	O-INT-NUC_-121022/4364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: SbPei SHA256: d827182e5f9b7a9ff0b9d3e232f7cfac43b5237e2681e11f005be627a49283a9 Module GUID: c1fbd624-27ea-40d1-aa48-94c3dc5c7e0d **CVE ID : CVE-2022-40246**		
Affected Version(s): bc0074					
Out-of-bounds Write	20-Sep-2022	8.8	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware	https://www.ami.com/security-center/	O-INT-NUC_-121022/4365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: SmmSmbiosElog SHA256: 3a8acb4f9bddccb19ec3b22b22ad97963711550f76b27b606461cd5073a93b59 Module GUID: 8e61fd6b-7a8b-404f-b83f-aa90a47cabdf This issue affects: AMI Aptio 5.x. This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-40250**		
Product: nuc_m15_laptop_kit_lapbc710_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: PlatformInitAdvancedPreMem SHA256: 644044fdb8daea30a7820e0f5f88dbf5cd460af72fbf70418e9d2e47efed8d9b Module GUID: EEEE611D-F78F-4FB9-B868-55907F169280 This issue affects: AMI Aptio 5.x.	https://www.ami.com/security-center/	O-INT-NUC_-121022/4366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26873		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Sep-2022	8.2	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some	https://www.ami.com/security-center/	O-INT-NUC_-121022/4367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			types of memory isolation for hypervisors). This issue affects: Module name: OverClockSmiHandler SHA256: a204699576e1a48ce915d9d9423380c8e4c197003baf9d17e6504f0265f3039c Module GUID: 4698C2BD-A903-410E-AD1F-5EEF3A1AE422 **CVE ID : CVE-2022-40261**		
Affected Version(s): 0072					
Out-of-bounds Write	20-Sep-2022	7.2	An attacker with physical access can exploit this vulnerability to execute arbitrary code during DXE phase. A malicious code installed as a result of vulnerability exploitation in DXE driver could survive across an operating system (OS) boot process and runtime This issue affects: Module name: AMITSE SHA256: 288769fcb374d9280735e259c579e2dc209491f4da43b085d6aabc2d6e6ee57d Module GUID: b1da0adf-4f77-	https://www.ami.com/security-center/	O-INT-NUC_-121022/4368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4070-a88e-bffe1c60529a This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-2154**		
Out-of-bounds Write	20-Sep-2022	7.2	A potential attacker can write one byte by arbitrary address at the time of the PEI phase (only during S3 resume boot mode) and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure, discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: SbPei SHA256: d827182e5f9b7a9ff0b9d3e232f7cfac43b5237e2681e11f005be627a49283a	https://www.ami.com/security-center/	O-INT-NUC_-121022/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9 Module GUID: c1fbd624-27ea-40d1-aa48-94c3dc5c7e0d **CVE ID : CVE-2022-40246**		
Affected Version(s): bc0074					
Out-of-bounds Write	20-Sep-2022	8.8	An attacker can exploit this vulnerability to elevate privileges from ring 0 to ring -2, execute arbitrary code in System Management Mode - an environment more privileged than operating system (OS) and completely isolated from it. Running arbitrary code in SMM additionally bypasses SMM-based SPI flash protections against modifications, which can help an attacker to install a firmware backdoor/implant into BIOS. Such a malicious firmware code in BIOS could persist across operating system re-installs. Additionally, this vulnerability potentially could be used by malicious actors to	https://www.ami.com/security-center/	O-INT-NUC_-121022/4370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass security mechanisms provided by UEFI firmware (for example, Secure Boot and some types of memory isolation for hypervisors). This issue affects: Module name: SmmSmbiosElog SHA256: 3a8acb4f9bddccb19ec3b22b22ad97963711550f76b27b606461cd5073a93b59 Module GUID: 8e61fd6b-7a8b-404f-b83f-aa90a47cabdf This issue affects: AMI Aptio 5.x. This issue affects: AMI Aptio 5.x. **CVE ID : CVE-2022-40250**		
Product: server_board_m10jnp2sb_firmware					
Affected Version(s): -					
Out-of-bounds Write	20-Sep-2022	8.2	A potential attacker can execute an arbitrary code at the time of the PEI phase and influence the subsequent boot stages. This can lead to the mitigations bypassing, physical memory contents disclosure,	https://www.ami.com/security-center/	O-INT-SERV-121022/4371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovery of any secrets from any Virtual Machines (VMs) and bypassing memory isolation and confidential computing boundaries. Additionally, an attacker can build a payload which can be injected into the SMRAM memory. This issue affects: Module name: S3Resume2Pei SHA256: 7bb29f05534a8a1e010443213451425098faebd45948a4642db969b19d0253fc Module GUID: 89E549B0-7CFE-449D-9BA3-10D8B2312D71 **CVE ID : CVE-2022-40262**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Privilege Management	16-Sep-2022	9.8	An issue in the component post_applogin.php of Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below allows attackers to escalate privileges	N/A	O-LIN-LINU-121022/4372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via creating crafted session tokens. **CVE ID : CVE-2022-36536**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Sep-2022	9.8	NuProcess is an external process execution implementation for Java. In all the versions of NuProcess where it forks processes by using the JVM's Java_java_lang_UNIXProcess_forkAndExec method (1.2.0+), attackers can use NUL characters in their strings to perform command line injection. Java's ProcessBuilder isn't vulnerable because of a check in ProcessBuilder.start. NuProcess is missing that check. This vulnerability can only be exploited to inject command line arguments on Linux. Version 2.0.5 contains a patch. As a workaround, users of the library can sanitize command strings to remove NUL characters prior to passing	https://github.com/brettwoodridge/NuProcess/commit/29bc09de561bf00ff9bf77123756363a9709f868, https://github.com/brettwoodridge/NuProcess/security/advisories/GHSA-cxgf-v2p8-7ph7, https://github.com/brettwoodridge/NuProcess/pull/143	O-LIN-LINU-121022/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			them to NuProcess for execution. **CVE ID : CVE-2022-39243**		
Use After Free	26-Sep-2022	8.8	Use after free in FedCM in Google Chrome prior to 104.0.5112.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2852**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html, https://crbug.com/1349322	O-LIN-LINU-121022/4374
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3196**	https://crbug.com/1358090, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html	O-LIN-LINU-121022/4375
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3197**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1358075	O-LIN-LINU-121022/4376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	8.8	Use after free in PDF in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-3198**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1355682	O-LIN-LINU-121022/4377
Use After Free	26-Sep-2022	8.8	Use after free in Frames in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3199**	https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html, https://crbug.com/1355237	O-LIN-LINU-121022/4378
Out-of-bounds Write	26-Sep-2022	8.8	Heap buffer overflow in Internals in Google Chrome prior to 105.0.5195.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-3200**	https://crbug.com/1355103, https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop_14.html	O-LIN-LINU-121022/4379
Improper Neutralization of Special Elements	16-Sep-2022	8.8	Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below was	N/A	O-LIN-LINU-121022/4380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			discovered to contain multiple remote code execution (RCE) vulnerabilities via the Job_ExecuteBefore and Job_ExecuteAfter parameters at post_profilesettings.php. **CVE ID : CVE-2022-36534**		
Use After Free	16-Sep-2022	7.8	There exists a use-after-free in io_uring in the Linux kernel. Signalfd_poll() and binder_poll() use a waitqueue whose lifetime is the current task. It will send a POLLFREE notification to all waiters before the queue is freed. Unfortunately, the io_uring poll doesn't handle POLLFREE. This allows a use-after-free to occur if a signalfd or binder fd is polled with io_uring poll, and the waitqueue gets freed. We recommend upgrading past commit fc78b2fc21f10c4c9	https://kernel.dance/#fc78b2fc21f10c4c9c4d5d659a685710ffa63659, https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit?h=linux-5.4.y&id=fc78b2fc21f10c4c9c4d5d659a685710ffa63659	O-LIN-LINU-121022/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c4d5d659a685710ffa63659 **CVE ID : CVE-2022-3176**		
Improper Input Validation	23-Sep-2022	5.5	IBM Common Cryptographic Architecture (CCA 5.x MTM for 4767 and CCA 7.x MTM for 4769) could allow a local user to cause a denial of service due to improper input validation. IBM X-Force ID: 223596. **CVE ID : CVE-2022-22423**	https://exchange.xforce.ibmcloud.com/vulnerabilities/223596, https://www.ibm.com/support/pages/node/6695893	O-LIN-LINU-121022/4382
Integer Overflow or Wraparound	16-Sep-2022	5.5	An integer overflow vulnerability was found in vmwgfx driver in drivers/gpu/vmxgfx/vmxgfx_execbuf.c in GPU component of Linux kernel with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS). **CVE ID : CVE-2022-36402**	N/A	O-LIN-LINU-121022/4383
Improper Neutralizat	23-Sep-2022	5.4	IBM Jazz for Service	https://www.ibm.com/support	O-LIN-LINU-121022/4384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Management 1.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 231380. **CVE ID : CVE-2022-35721**	/pages/node/6695811, https://exchange.xforce.ibmcloud.com/vulnerabilities/231380	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Sep-2022	5.4	Super Flexible Software GmbH & Co. KG Syncovery 9 for Linux v9.47x and below was discovered to contain a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-36533**	N/A	O-LIN-LINU-121022/4385
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://exchange.xforce.ibmcloud.com/vulnerabilities/236586, https://www.ibm.com/support/pages/node/6695961	O-LIN-LINU-121022/4386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236586. **CVE ID : CVE-2022-40748**		
Affected Version(s): * Up to (excluding) 2022-08-10					
Out-of-bounds Read	23-Sep-2022	5.5	There exists an arbitrary memory read within the Linux Kernel BPF - Constants provided to fill pointers in structs passed in to bpf_sys_bpf are not verified and can point anywhere, including memory not owned by BPF. An attacker with CAP_BPF can arbitrarily read memory from anywhere on the system. We recommend upgrading past commit 86f44fcec22c **CVE ID : CVE-2022-2785**	https://git.kernel.org/bpf/bpf/c/86f44fcec22c, https://lore.kernel.org/bpf/20220816205517.682470-1-zhuyifei@google.com/T/#t	O-LIN-LINU-121022/4387
Affected Version(s): * Up to (excluding) 5.13.3					
Use After Free	21-Sep-2022	4.7	mm/mremap.c in the Linux kernel before 5.13.3 has a use-after-free via a stale TLB because an rmap lock is not	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.3, https://bugs.chromium.org/p/	O-LIN-LINU-121022/4388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			held during a PUD move. **CVE ID : CVE-2022-41222**	project-zero/issues/detail?id=2347, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=97113eb39fa7972722ff490b947d8af023e1f6a2	
Affected Version(s): * Up to (excluding) 6.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-Sep-2022	4.7	A race condition flaw was found in the Linux kernel sound subsystem due to improper locking. It could lead to a NULL pointer dereference while handling the SNDCTL_DSP_SYNC ioctl. A privileged local user (root or member of the audio group) could use this flaw to crash the system, resulting in a denial of service condition **CVE ID : CVE-2022-3303**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d, https://lore.kernel.org/all/CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/	O-LIN-LINU-121022/4389
Affected Version(s): * Up to (including) 5.19.10					
Use After Free	21-Sep-2022	5.5	In drivers/media/dvb-core/dmxdev.c in the Linux kernel through 5.19.10, there is a use-after-free caused by	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/log/drivers/media/dvb-core/dmxdev.c,	O-LIN-LINU-121022/4390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refcount races, affecting dvb_demux_open and dvb_dmxdev_release. **CVE ID : CVE-2022-41218**	https://lore.kernel.org/all/20220908132754.30532-1-tiwai@suse.de/	
Affected Version(s): * Up to (including) 5.19.9					
Exposure of Resource to Wrong Sphere	18-Sep-2022	5.5	drivers/scsi/stex.c in the Linux kernel through 5.19.9 allows local users to obtain sensitive information from kernel memory because stex_queuecommand_lck lacks a memset for the PASSTHRU_CMD case. **CVE ID : CVE-2022-40768**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/log/drivers/scsi/stex.c, https://www.openwall.com/lists/oss-security/2022/09/09/1, https://lore.kernel.org/all/20220908145154.2284098-1-gregkh@linuxfoundation.org/	O-LIN-LINU-121022/4391
Affected Version(s): 5.18					
Use After Free	19-Sep-2022	7.8	A flaw use after free in the Linux kernel video4linux driver was found in the way user triggers em28xx_usb_probe() for the Empia 28xx based TV cards. A local user could use this flaw to crash the system or potentially escalate their	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c08eadca1bdfa099e20a32f8fa4b52b2f672236d	O-LIN-LINU-121022/4392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on the system. **CVE ID : CVE-2022-3239**		
Affected Version(s): 6.0					
Off-by-one Error	26-Sep-2022	7.8	off-by-one in io_uring module. **CVE ID : CVE-2022-3103**	N/A	O-LIN-LINU-121022/4393
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-Sep-2022	4.7	A race condition flaw was found in the Linux kernel sound subsystem due to improper locking. It could lead to a NULL pointer dereference while handling the SNDCTL_DSP_SYNC ioctl. A privileged local user (root or member of the audio group) could use this flaw to crash the system, resulting in a denial of service condition **CVE ID : CVE-2022-3303**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d, https://lore.kernel.org/all/CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/	O-LIN-LINU-121022/4394
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory	19-Sep-2022	9.8	This vulnerability of SecureGate is SQL-Injection using login without password. A path traversal vulnerability is also	N/A	O-MIC-WIND-121022/4395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			identified during file transfer. An attacker can take advantage of these vulnerabilities to perform various attacks such as obtaining privileges and executing remote code, thereby taking over the victim's system. **CVE ID : CVE-2022-23767**		
Improper Authentication	19-Sep-2022	9.8	A vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service could allow an attacker to bypass the product's login authentication by falsifying request parameters on affected installations. **CVE ID : CVE-2022-40144**	https://www.ipa.go.jp/security/ciadr/vul/20220913-jvn.html, https://success.trendmicro.com/solution/000291528, https://appweb.trendmicro.com/SupportNews/NewsDetail.aspx?id=4553, https://jvn.jp/en/jp/JVN36454862/index.html	O-MIC-WIND-121022/4396
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Sep-2022	8.8	An improper input validation vulnerability leading to arbitrary file execution was discovered in BigFileAgent. In order to cause arbitrary files to be executed, the attacker makes the victim access a web	N/A	O-MIC-WIND-121022/4397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page d by them or inserts a script using XSS into a general website. **CVE ID : CVE-2022-23766**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28852**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4398
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28853		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38416**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4400
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38417**		
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38426**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4402
Access of Uninitialized Pointer	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38427**		
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35700**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4404
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38429**		
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38430**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4406
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an	https://helpx.adobe.com/security/products/p	O-MIC-WIND-121022/4407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38431**	hotoshop/apsb22-52.html	
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38432**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.sue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38433**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4409
Improper Link Resolution Before File Access ('Link Following')	19-Sep-2022	7.8	Trend Micro Security 2022 (consumer) has a link following vulnerability where an attacker with lower privileges could manipulate a mountpoint which could lead to escalation of privilege on an affected machine. **CVE ID : CVE-2022-34893**	https://helpcenter.trendmicro.com/en-us/article/tmka-11053	O-MIC-WIND-121022/4410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35699**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4411
Use After Free	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38434**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4412
Out-of-bounds Write	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-	https://helpx.adobe.com/security/products/br	O-MIC-WIND-121022/4413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35701**	idge/apsb22-49.html	
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35702**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35703**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4415
Use After Free	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35704		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35705**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4417
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35706**		
Out-of-bounds Read	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35707**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4419
Heap-based Buffer Overflow	19-Sep-2022	7.8	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35708**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38404**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4421
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-35713**		
Incorrect Default Permissions	19-Sep-2022	7.8	A vulnerability on Trend Micro HouseCall version 1.62.1.1133 and below could allow a local attacker to escalate privlieges due to an overly permissive folder om the product installer. **CVE ID : CVE-2022-38764**	https://helpcenter.trendmicro.com/en-us/article/tmka-11092	O-MIC-WIND-121022/4423
Improper Privilege Management	19-Sep-2022	7.8	A security link following local privilege escalation vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service agents could allow a local attacker to create a writable folder in an arbitrary location and escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	https://success.trendmicro.com/solution/000291528	O-MIC-WIND-121022/4424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40142		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38401**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4425
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38402**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38403**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4427
Out-of-bounds Read	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/animate/apsb22-54.html	O-MIC-WIND-121022/4428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-38412**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38405**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4429
Improper Input Validation	16-Sep-2022	7.8	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. requires user	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	O-MIC-WIND-121022/4430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38408**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe Animate version 21.0.11 (and earlier) and 22.0.7 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38411**	https://helpx.adobe.com/security/products/animate/apsb22-54.html	O-MIC-WIND-121022/4431
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-38413**		
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38414**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4433
Out-of-bounds Write	16-Sep-2022	7.8	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38415		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Sep-2022	7.5	Hertz v0.3.0 ws discovered to contain a path traversal vulnerability via the normalizePath function. **CVE ID : CVE-2022-40082**	https://github.com/cloudwego/hertz/pull/229	O-MIC-WIND-121022/4435
Inadequate Encryption Strength	19-Sep-2022	7.5	A vulnerability in Trend Micro Apex One and Apex One as a Service could allow an attacker to intercept and decode certain communication strings that may contain some identification attributes of a particular Apex One server. **CVE ID : CVE-2022-40141**	https://success.trendmicro.com/solution/000291528	O-MIC-WIND-121022/4436
Improper Link Resolution Before File Access ('Link Following')	19-Sep-2022	7.3	A link following local privilege escalation vulnerability in Trend Micro Apex One and Trend Micro Apex One as a Service servers could allow a local attacker to abuse an insecure directory that could allow a low-privileged user to run arbitrary code	https://success.trendmicro.com/solution/000291528	O-MIC-WIND-121022/4437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with elevated privileges. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40143**		
Improper Input Validation	19-Sep-2022	7.2	Improper validation of some components used by the rollback mechanism in Trend Micro Apex One and Trend Micro Apex One as a Service clients could allow a Apex One server administrator to instruct affected clients to download an unverified rollback package, which could lead to remote code execution. Please note: an attacker must first obtain Apex One server administration console access in order to exploit this vulnerability. **CVE ID : CVE-2022-40139**	https://success.trendmicro.com/solution/000291528	O-MIC-WIND-121022/4438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28854**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4439
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28855		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-28856**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4441
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a victim must open a malicious file. **CVE ID : CVE-2022-28857**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30672**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4443
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30673**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30674**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4445
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30675**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30676**	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4447
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InDesign versions 16.4.2 (and earlier) and 17.3 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/indesign/apsb22-50.html	O-MIC-WIND-121022/4448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-30671**		
Out-of-bounds Read	19-Sep-2022	5.5	Trend Micro Security 2021 and 2022 (Consumer) is vulnerable to an Out-Of-Bounds Read Information Disclosure Vulnerability that could allow an attacker to read sensitive information from other memory locations and cause a crash on an affected machine. This vulnerability is similar to, but not the same as CVE-2022-35234. **CVE ID : CVE-2022-37347**	https://helpcenter.trendmicro.com/en-us/article/tmka-11058	O-MIC-WIND-121022/4449
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38407**		
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35709**	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4451
Use After Free	19-Sep-2022	5.5	Adobe Bridge version 12.0.2 (and earlier) and 11.1.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/bridge/apsb22-49.html	O-MIC-WIND-121022/4452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38425**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe InCopy version 17.3 (and earlier) and 16.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38406**	https://helpx.adobe.com/security/products/incopy/apsb22-53.html	O-MIC-WIND-121022/4453
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	O-MIC-WIND-121022/4454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38409**		
Use After Free	16-Sep-2022	5.5	Adobe Photoshop versions 22.5.8 (and earlier) and 23.4.2 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38428**	https://helpx.adobe.com/security/products/photoshop/apsb22-52.html	O-MIC-WIND-121022/4455
Origin Validation Error	19-Sep-2022	5.5	An origin validation error vulnerability in Trend Micro Apex One and Apex One as a Service could allow a local attacker to cause a denial-of-service on affected installations.	https://success.trendmicro.com/solution/000291528	O-MIC-WIND-121022/4456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2022-40140**		
Out-of-bounds Read	16-Sep-2022	5.5	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-38410**	https://helpx.adobe.com/security/products/illustrator/apsb22-55.html	O-MIC-WIND-121022/4457
Out-of-bounds Read	19-Sep-2022	5.5	Trend Micro Security 2021 and 2022 (Consumer) is vulnerable to an Out-Of-Bounds Read Information Disclosure Vulnerability that could allow an attacker to read sensitive	https://helpcenter.trendmicro.com/en-us/article/tmka-11058	O-MIC-WIND-121022/4458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information from other memory locations and cause a crash on an affected machine. This vulnerability is similar to, but not the same as CVE-2022-37347. **CVE ID : CVE-2022-37348**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	IBM Jazz for Service Management 1.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 231380. **CVE ID : CVE-2022-35721**	https://www.ibm.com/support/pages/node/6695811, https://exchange.xforce.ibmcloud.com/vulnerabilities/231380	O-MIC-WIND-121022/4459
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Sep-2022	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus	https://exchange.xforce.ibmcloud.com/vulnerabilities/236586, https://www.ibm.com/support/pages/node/6695961	O-MIC-WIND-121022/4460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 236586. **CVE ID : CVE-2022-40748**		
Vendor: mipcm					
Product: mipc_camera_firmware					
Affected Version(s): 5.3.1.2003161406					
Out-of-bounds Write	26-Sep-2022	8.8	Unlimited strcpy on user input when setting a locale file leads to stack buffer overflow in mIPC camera firmware 5.3.1.2003161406. **CVE ID : CVE-2022-40784**	N/A	O-MIP-MIPC-121022/4461
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Sep-2022	8.8	Unsanitized input when setting a locale file leads to shell injection in mIPC camera firmware 5.3.1.2003161406. This allows an attacker to gain remote code execution on cameras running the firmware when a victim logs into a specially crafted mobile app.	N/A	O-MIP-MIPC-121022/4462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40785		
Vendor: neoinfosys					
Product: nis-hap11ac_firmware					
Affected Version(s): 3.0					
N/A	19-Sep-2022	9.8	This Vulnerability in NIS-HAP11AC is caused by an exposed external port for the telnet service. Remote attackers use this vulnerability to induce all attacks such as source code hijacking, remote control of the device. **CVE ID : CVE-2022-23768**	N/A	O-NEO-NIS--121022/4463
Vendor: Netgear					
Product: r7000_firmware					
Affected Version(s): 1.0.11.134_10.2.119					
Out-of-bounds Write	23-Sep-2022	9.8	Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncat **CVE ID : CVE-2022-37235**	https://www.netgear.com/about/security/, https://www.netgear.com/support/download/?model=R7000	O-NET-R700-121022/4464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-Sep-2022	7.8	Netgear Nighthawk AC1900 Smart WiFi Dual Band Gigabit Router R7000-V1.0.11.134_10.2.119 is vulnerable to Buffer Overflow via the wl binary in firmware. There is a stack overflow vulnerability caused by strncpy. **CVE ID : CVE-2022-37234**	https://www.netgear.com/about/security/, https://www.netgear.com/support/download/?model=R7000	O-NET-R700-121022/4465
Product: wnr2000v4_firmware					
Affected Version(s): 1.0.0.70					
Out-of-bounds Write	22-Sep-2022	9.8	Netgear N300 wireless router wnr2000v4-V1.0.0.70 was discovered to contain a stack overflow via strcpy in uhttpd. **CVE ID : CVE-2022-31937**	https://www.netgear.com/support/download/?model=WNR2000v4, https://www.netgear.com/about/security/	O-NET-WNR2-121022/4466
Out-of-bounds Write	23-Sep-2022	9.8	Netgear N300 wireless router wnr2000v4-V1.0.0.70 is vulnerable to Buffer Overflow via uhttpd. There is a stack overflow vulnerability caused by strcpy. **CVE ID : CVE-2022-37232**	https://www.netgear.com/about/security/	O-NET-WNR2-121022/4467
Product: wpn824ext_firmware					
Affected Version(s): * Up to (including) 1.1.1_1.1.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	20-Sep-2022	5.3	An exploitable firmware downgrade vulnerability was discovered on the Netgear WPN824EXT WiFi Range Extender. An attacker can conduct a MITM attack to replace the user-uploaded firmware image with an original old firmware image. This affects Firmware 1.1.1_1.1.9 and earlier. **CVE ID : CVE-2022-38956**	https://www.netgear.com/about/security/	O-NET-WPN8-121022/4468
Affected Version(s): 1.1.1_1.1.9					
Improper Validation of Integrity Check Value	20-Sep-2022	7.5	An exploitable firmware modification vulnerability was discovered on the Netgear WPN824EXT WiFi Range Extender. An attacker can conduct a MITM attack to modify the user-uploaded firmware image and bypass the CRC check. A successful attack can either introduce a backdoor to the device or make the device DoS. This affects Firmware	https://www.netgear.com/about/security/	O-NET-WPN8-121022/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Version: 1.1.1_1.1.9. **CVE ID : CVE-2022-38955**		
Vendor: Opensuse					
Product: tumbleweed					
Affected Version(s): -					
Incorrect Authorization	19-Sep-2022	9.8	The Linux-PAM package before 1.5.2-6.1 for openSUSE Tumbleweed allows authentication bypass for SSH logins. The pam_access.so module doesn't correctly restrict login if a user tries to connect from an IP address that is not resolvable via DNS. In such conditions, a user with denied access to a machine can still get access. NOTE: the relevance of this issue is largely limited to openSUSE Tumbleweed and openSUSE Factory; it does not affect Linux-PAM upstream. **CVE ID : CVE-2022-28321**	https://www.suse.com/security/cve/CVE-2022-28321.html, http://download.opensuse.org/source/distribution/openSUSE-current/repo/oss/src/, https://bugzilla.suse.com/show_bug.cgi?id=1197654	O-OPE-TUMB-121022/4470
Vendor: Qualcomm					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: apq8009w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4471
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-APQ8-121022/4472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4473
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4475
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: apq8009_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-APQ8-121022/4479
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-APQ8-121022/4480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4481
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-APQ8-121022/4482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Product: apq8017_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4483
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-APQ8-121022/4484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4485
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-APQ8-121022/4486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4488
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4490
Product: apq8053_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-APQ8-121022/4494
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4496
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4498
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4500
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4502
Product: apq8096au_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4504
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-APQ8-121022/4505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4506
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4508
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-APQ8-121022/4510
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input	https://www.qualcomm.com/company/product-	O-QUA-APQ8-121022/4511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	security/bulletins/september-2022-bulletin	
Product: aqt1000_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4512
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-AQT1-121022/4514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4515
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4517
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4519
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4521
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4523
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AQT1-121022/4525
Product: ar8031_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4527
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4529
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4531
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: ar8035_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4533
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	O-QUA-AR80-121022/4534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4535
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4537
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4539
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-AR80-121022/4541
Product: csr8811_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSR8-121022/4542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: csra6620_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4545
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4547
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4549
Product: csra6640_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-CSRA-121022/4550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4551
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4553
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRA-121022/4555
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	O-QUA-CSRA-121022/4556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Product: csrb31024_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRB-121022/4557
Use After Free	26-Sep-2022	7.8	Memory corruption due to	https://www.qualcomm.com/c	O-QUA-CSRB-121022/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ompany/product-security/bulletins/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRB-121022/4559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRB-121022/4560
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRB-121022/4561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-CSRB-121022/4562
Product: ipq5010_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ5-121022/4563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: ipq5018_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ5-121022/4564
Product: ipq5028_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ5-121022/4565
Product: ipq6000_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ6-121022/4566
Product: ipq6005_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ6-121022/4567
Product: ipq6010_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ6-121022/4568
Product: ipq6018_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ6-121022/4569
Product: ipq6028_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ6-121022/4570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: ipq8070a_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4571
Product: ipq8070_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4572
Product: ipq8071a_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4573
Product: ipq8071_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4574
Product: ipq8072a_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4575
Product: ipq8072_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4576
Product: ipq8074a_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ8-121022/4577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: ipq8074_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4578
Product: ipq8076a_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4579
Product: ipq8076_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4580
Product: ipq8078a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4581
Product: ipq8078_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4582
Product: ipq8173_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-IPQ8-121022/4583
Product: ipq8174_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-IPQ8-121022/4584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: mdm9150_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4585
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4587
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Product: mdm9206_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4589
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4592
Product: mdm9250_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4593
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	O-QUA-MDM9-121022/4594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22058		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4596
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4598
Product: mdm9607_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4600
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4602
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4604
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MDM9-121022/4605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Product: mdm9626_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4606
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MDM9-121022/4607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22058		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4609
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4611
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: mdm9628_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4615
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MDM9-121022/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4617
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MDM9-121022/4618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: mdm9640_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4620
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4622
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4624
Product: mdm9650_firmware					
Affected Version(s): -					
Integer Overflow	16-Sep-2022	9.8	Memory corruption in	https://www.qualcomm.com/c	O-QUA-MDM9-121022/4625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ompany/product-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4626
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MDM9-121022/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4629
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4631
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MDM9-121022/4632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Product: msm8909w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4633
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MSM8-121022/4634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4635
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MSM8-121022/4636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4638
Product: msm8917_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4640
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MSM8-121022/4641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4642
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4644
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: msm8920_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4646
Product: msm8937_firmware					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while	https://www.qualcomm.com/company/product-	O-QUA-MSM8-121022/4647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	security/bulletins/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4649
Product: msm8940_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Product: msm8953_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4651
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MSM8-121022/4653
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MSM8-121022/4654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4655
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4657
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4659
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MSM8-121022/4660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4661
Product: msm8996au_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-MSM8-121022/4662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-MSM8-121022/4663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4664
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4666
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-MSM8-121022/4667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: pm8937_firmware					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-PM89-121022/4668
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-PM89-121022/4669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-PM89-121022/4670
Product: pmp8074_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-PMP8-121022/4671
Product: qca1062_firmware					
Affected Version(s): -					
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA1-121022/4672
Product: qca1064_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA1-121022/4673
Product: qca4020_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA4-121022/4674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA4-121022/4675
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA4-121022/4676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA4-121022/4677
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA4-121022/4678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA4-121022/4679
Product: qca4024_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA4-121022/4680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qca6174a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4683
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4685
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4687
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4689
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4691
Product: qca6175a_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4692
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4694
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca6310_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4697
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4699
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4701
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: qca6320_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4703
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4706
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4708
Product: qca6335_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4710
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4712
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4714
Product: qca6390_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4715
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4717
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4719
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4720
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4722
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4725
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4727
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4728
Time-of-check	16-Sep-2022	7	Memory corruption in	https://www.qualcomm.com/c	O-QUA-QCA6-121022/4729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4730
Product: qca6391_firmware					
Affected Version(s): -					
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video module due to	https://www.qualcomm.com/company/produc	O-QUA-QCA6-121022/4731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	t-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4732
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4735
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4736
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4738
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4740
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4743
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4744
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4746
Product: qca6420_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4748
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4750
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	O-QUA-QCA6-121022/4751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4753
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4755
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4757
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22094		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4759
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4760
Product: qca6421_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4761
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4763
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4764
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-QCA6-121022/4765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4767
Product: qca6426_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4768
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	O-QUA-QCA6-121022/4769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4771
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4772
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4774
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4776
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4779
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4781
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4782
Product: qca6428_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qca6430_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4786
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4788
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4790
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4793
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4795
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4796
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: qca6431_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4798
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	O-QUA-QCA6-121022/4799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4800
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4802
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	O-QUA-QCA6-121022/4803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4804
Product: qca6436_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4806
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4808
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4810
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4812
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4814
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4816
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4818
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: qca6438_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4820
Product: qca6564au_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4821
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4824
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4826
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4828
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4830
Product: qca6564a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4832
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4834
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	O-QUA-QCA6-121022/4835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4837
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4839
Product: qca6564_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4841
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6574au_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4844
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4845
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4848
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4850
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4852
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4854
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4856
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Product: qca6574a_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4858
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4860
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4862
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4864
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4866
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4869
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: qca6574_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4871
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4873
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4875
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4877
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4879
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4882
Product: qca6584_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4883
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4886
Product: qca6595au_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4888
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4890
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4892
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4894
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4896
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4898
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4900
Product: qca6595_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA6-121022/4901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4902
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca6694_firmware					
Affected Version(s): -					
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca6696_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4905
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4907
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA6-121022/4908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4909
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4911
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4913
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4916
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA6-121022/4917
Product: qca8072_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4918
Product: qca8075_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4919
Product: qca8081_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4921
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4923
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4924
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4925
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA8-121022/4926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	ns/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4928
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: qca8337_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4930
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA8-121022/4931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4932
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22089		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4934
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4935
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	O-QUA-QCA8-121022/4936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25670		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA8-121022/4938
Product: qca9367_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4940
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA9-121022/4941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4942
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4944
Product: qca9377_firmware					
Affected Version(s): -					
Integer Overflow or	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow	https://www.qualcomm.com/company/product-	O-QUA-QCA9-121022/4945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4946
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA9-121022/4947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4949
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4951
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4953
Product: qca9379_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4955
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCA9-121022/4956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4957
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4959
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCA9-121022/4960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Product: qca9888_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4961
Product: qca9889_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCA9-121022/4962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25652		
Product: qcm2290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4965
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4967
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4969
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4971
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM2-121022/4972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: qcm4290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4975
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCM4-121022/4976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4977
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4979
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4982
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM4-121022/4984
Product: qcm6125_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4986
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4988
Product: qcm6490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4990
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4992
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4994
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4996
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4998
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/4999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCM6-121022/5000
Product: qcn5021_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5001
Product: qcn5022_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN5-121022/5002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qcn5024_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5003
Product: qcn5052_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5004
Product: qcn5054_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5005
Product: qcn5064_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5006
Product: qcn5121_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5007
Product: qcn5122_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5008
Product: qcn5124_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN5-121022/5009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qcn5152_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5010
Product: qcn5154_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5011
Product: qcn5164_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5012
Product: qcn5550_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN5-121022/5013
Product: qcn6023_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN6-121022/5014
Product: qcn6024_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN6-121022/5015
Product: qcn6100_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCN6-121022/5016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2022-25652**	ns/september-2022-bulletin	
Product: qcn6102_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN6-121022/5017
Product: qcn6112_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN6-121022/5018
Product: qcn6122_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN6-121022/5019
Product: qcn6132_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN6-121022/5020
Product: qcn7605_firmware					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCN7-121022/5021
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-QCN7-121022/5022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Product: qcn7606_firmware					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCN7-121022/5023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN7-121022/5024
Product: qcn9000_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash	https://www.qualcomm.com/company/produc	O-QUA-QCN9-121022/5025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	t-security/bulletins/september-2022-bulletin	
Product: qcn9012_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN9-121022/5026
Product: qcn9022_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN9-121022/5027
Product: qcn9024_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN9-121022/5028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9070_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN9-121022/5029
Product: qcn9072_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN9-121022/5030
Product: qcn9074_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCN9-121022/5031
Product: qcn9100_firmware					
Affected Version(s): -					
Improper Authentication	16-Sep-2022	7.8	Cryptographic issues in BSP due to improper hash verification in	https://www.qualcomm.com/company/product-	O-QUA-QCN9-121022/5032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2022-25652**	security/bulletins/september-2022-bulletin	
Product: qcs2290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5033
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5035
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5037
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5039
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS2-121022/5041
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS2-121022/5042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Product: qcs405_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5045
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5047
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Product: qcs410_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5050
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5052
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5054
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5056
Product: qcs4290_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5058
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5060
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS4-121022/5061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	ns/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5062
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5064
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS4-121022/5065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5067
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS4-121022/5068
Product: qcs603_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCS6-121022/5069
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5071
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5073
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5075
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: qcs605_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5077
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QCS6-121022/5078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5079
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS6-121022/5080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5081
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS6-121022/5082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5084
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25654		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5086
Product: qcs610_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5088
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5090
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5092
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5094
Product: qcs6125_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5096
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QCS6-121022/5097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs6490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5101
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5102
Integer Overflow or	16-Sep-2022	7.8	Possible integer overflow and memory	https://www.qualcomm.com/company/produc	O-QUA-QCS6-121022/5103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5105
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5107
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5108
Time-of-check	16-Sep-2022	7	Memory corruption in	https://www.qualcomm.com/c	O-QUA-QCS6-121022/5109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QCS6-121022/5110
Product: qrb5165m_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing	https://www.qualcomm.com/company/produc	O-QUA-QRB5-121022/5111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	t-security/bulletins/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5113
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5114
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5116
Time-of-check Time-of-	16-Sep-2022	7	Memory corruption or temporary denial	https://www.qualcomm.com/company/produc	O-QUA-QRB5-121022/5117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	t-security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5118
Product: qrb5165n_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5120
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-QRB5-121022/5121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5122
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5124
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5126
Product: qrb5165_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5128
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5130
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5132
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QRB5-121022/5134
Product: qsm8350_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QSM8-121022/5135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QSM8-121022/5136
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QSM8-121022/5137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QSM8-121022/5138
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QSM8-121022/5139
Product: qualcomm215_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5140
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-QUAL-121022/5142
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5144
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5146
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5148
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-QUAL-121022/5150
Product: sa415m_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA41-121022/5151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SA41-121022/5152
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA41-121022/5153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA41-121022/5154
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA41-121022/5155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA41-121022/5156
Product: sa515m_firmware					
Affected Version(s): -					
Integer Overflow or	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow	https://www.qualcomm.com/company/product-	O-QUA-SA51-121022/5157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA51-121022/5158
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA51-121022/5159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA51-121022/5160
Product: sa6145p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5161
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5163
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5165
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5167
Product: sa6155p_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA61-121022/5168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5169
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5171
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5173
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5175
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5177
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5179
Product: sa6155_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5181
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5183
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5185
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA61-121022/5188
Product: sa8155p_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5189
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	O-QUA-SA81-121022/5190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5191
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-121022/5192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5194
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5195
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-121022/5196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5197
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-SA81-121022/5198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5200
Product: sa8155_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5201
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video module due to	https://www.qualcomm.com/company/produc	O-QUA-SA81-121022/5202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	t-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5203
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SA81-121022/5204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5206
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5208
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Product: sa8195p_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5210
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5212
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5214
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5216
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5218
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5220
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SA81-121022/5221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SC81-121022/5222
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SC81-121022/5223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SC81-121022/5224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd429_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5225
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD42-121022/5227
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5229
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5231
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5233
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD42-121022/5234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd439_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5235
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD43-121022/5237
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5239
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5241
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5243
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD43-121022/5244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: sd450_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD45-121022/5245
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD45-121022/5246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD45-121022/5247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD45-121022/5248
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD45-121022/5249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD45-121022/5250
Product: sd460_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5252
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5254
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5256
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5258
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5260
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD46-121022/5261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5262
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD46-121022/5263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd480_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5264
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5266
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD48-121022/5267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5268
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD48-121022/5269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5270
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD48-121022/5271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5273
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD48-121022/5274
Product: sd632_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD63-121022/5275
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD63-121022/5276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD63-121022/5277
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD63-121022/5278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD63-121022/5279
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD63-121022/5280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD63-121022/5281
Product: sd660_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5283
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD66-121022/5284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5285
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	O-QUA-SD66-121022/5286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5287
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to improper	https://www.qualcomm.com/company/product-	O-QUA-SD66-121022/5288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Product: sd662_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5292
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5294
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5296
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5298
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5300
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd665_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5302
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5304
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5306
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5308
Time-of-check Time-of-	16-Sep-2022	7	Memory corruption in display due to	https://www.qualcomm.com/company/produc	O-QUA-SD66-121022/5309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD66-121022/5310
Product: sd670_firmware					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	O-QUA-SD67-121022/5311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5312
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD67-121022/5313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5315
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5317
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Product: sd675_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5319
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5321
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5323
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5325
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5327
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption in display due to time-of-check time-	https://www.qualcomm.com/company/product-	O-QUA-SD67-121022/5328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5329
Product: sd678_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD67-121022/5330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5331
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD67-121022/5332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5333
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	O-QUA-SD67-121022/5334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5335
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	O-QUA-SD67-121022/5336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5338
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD67-121022/5340
Product: sd680_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5342
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5344
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22095		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5346
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5348
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5350
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD68-121022/5351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd690_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5352
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5354
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5356
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5358
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5360
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5362
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd695_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5366
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5368
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD69-121022/5369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5371
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD69-121022/5372
Product: sd710_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD71-121022/5375
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5377
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5379
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5381
Product: sd712_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD71-121022/5383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sd720g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5384
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25688		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5386
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5388
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5390
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD72-121022/5391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5392
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD72-121022/5393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd730_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5394
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5396
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5398
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD73-121022/5399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5400
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-SD73-121022/5401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5403
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD73-121022/5404
Product: sd750g_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5405
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5407
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5409
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5411
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5413
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5415
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD75-121022/5416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd765g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5417
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5419
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5421
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5423
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5425
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5427
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22094		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5429
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5430
Product: sd765_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5431
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5433
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5435
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5436
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5438
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5441
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5443
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5444
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD76-121022/5445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: sd768g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5446
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5448
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer	https://www.qualcomm.com/company/product-	O-QUA-SD76-121022/5449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5450
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5452
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5454
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD76-121022/5455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5456
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5458
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd768_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD76-121022/5460
Product: sd778g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5462
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5464
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5466
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5468
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5470
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5472
Product: sd778_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD77-121022/5473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Product: sd780g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5474
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5476
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5478
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5480
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5482
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5484
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5486
Product: sd780_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD78-121022/5487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Product: sd7c_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD7C-121022/5488
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD7C-121022/5489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD7C-121022/5490
Product: sd820_firmware					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD82-121022/5491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD82-121022/5492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD82-121022/5493
Product: sd835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD83-121022/5494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD83-121022/5495
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD83-121022/5496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD83-121022/5497
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD83-121022/5498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD83-121022/5499
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD83-121022/5500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Product: sd845_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD84-121022/5501
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue	https://www.qualcomm.com/company/produc	O-QUA-SD84-121022/5502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	t-security/bulletins/july-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD84-121022/5503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD84-121022/5504
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD84-121022/5505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD84-121022/5506
Product: sd850_firmware					
Affected Version(s): -					
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5508
Product: sd855_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SD85-121022/5511
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5513
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5515
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5517
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5519
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD85-121022/5521
Product: sd865_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5523
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5525
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5527
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5529
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5531
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5533
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5535
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD86-121022/5537
Product: sd870_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5539
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5541
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5542
Use After Free	16-Sep-2022	7.8	Memory corruption in synx	https://www.qualcomm.com/c	O-QUA-SD87-121022/5543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	ompany/product-security/bulletins/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5544
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD87-121022/5545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5546
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD87-121022/5547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5549
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5551
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD87-121022/5552
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-	https://www.qualcomm.com/company/produc	O-QUA-SD87-121022/5553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	t-security/bulletins/september-2022-bulletin	
Product: sd888_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5554
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD88-121022/5555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5556
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5558
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5560
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5562
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5564
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5566
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5568
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5570
Product: sd888_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5572
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5574
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5576
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5578
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5580
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5581
Time-of-check	16-Sep-2022	7	Memory corruption in	https://www.qualcomm.com/c	O-QUA-SD88-121022/5582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD88-121022/5583
Product: sdm429w_firmware					
Affected Version(s): -					
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video due to buffer	https://www.qualcomm.com/company/produc	O-QUA-SDM4-121022/5584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	t-security/bulletins/september-2022-bulletin	
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SDM4-121022/5585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM4-121022/5586
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM4-121022/5587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM4-121022/5588
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM4-121022/5589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25654		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM4-121022/5590
Product: sdm630_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM6-121022/5591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM6-121022/5592
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM6-121022/5593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM6-121022/5594
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM6-121022/5595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDM6-121022/5596
Product: sdw2500_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDW2-121022/5597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SDW2-121022/5598
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDW2-121022/5599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDW2-121022/5600
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDW2-121022/5601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDW2-121022/5602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sdx12_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX1-121022/5603
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX1-121022/5604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Product: sdx20_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5605
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SDX2-121022/5607
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5609
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5611
Product: sdx24_firmware					
Affected Version(s): -					
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue	https://www.qualcomm.com/company/produc	O-QUA-SDX2-121022/5612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	t-security/bulletins/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5614
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX2-121022/5615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Product: sdx50m_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5616
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5618
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5620
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDX5-121022/5621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5622
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sdx55m_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5626
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5628
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22095		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5630
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5632
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5634
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5636
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5638
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: sdx55_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5640
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5641
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	O-QUA-SDX5-121022/5642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5644
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5645
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	O-QUA-SDX5-121022/5646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5647
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	O-QUA-SDX5-121022/5648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5650
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX5-121022/5652
Product: sdx65_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5654
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5656
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5657
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5659
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDX6-121022/5661
Product: sdxr1_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5662
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-SDXR-121022/5663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5664
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5666
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5668
Product: sdxr2_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5670
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5672
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SDXR-121022/5673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5674
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5676
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5678
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5680
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5682
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SDXR-121022/5683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: sd_636_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5684
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5686
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5688
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5690
Product: sd_675_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5692
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5694
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD_6-121022/5695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5696
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD_6-121022/5697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5699
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_6-121022/5701
Product: sd_8cx_firmware					
Affected Version(s): -					
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5703
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Product: sd_8cx_gen2_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5705
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5707
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5709
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SD_8-121022/5710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	ns/september-2022-bulletin	
Product: sd_8cx_gen3_firmware					
Affected Version(s): -					
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5711
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5713
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	O-QUA-SD_8-121022/5714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5715
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5717
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5719
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5720
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5722
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5724
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5726
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5728
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5730
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SD_8-121022/5731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: sm4125_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5732
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5734
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5736
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5738
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5740
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM41-121022/5742
Product: sm6250p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5744
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM62-121022/5745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5746
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM62-121022/5747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5749
Product: sm6250_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5751
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5753
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5755
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5757
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM62-121022/5758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM62-121022/5759
Product: sm7250p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM72-121022/5760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5761
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5763
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM72-121022/5764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	ns/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5765
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5767
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5769
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5771
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5773
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM72-121022/5774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: sm7315_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5777
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5779
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5781
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5783
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5785
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5787
Product: sm7325p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5788
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	O-QUA-SM73-121022/5789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5791
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5792
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in	https://www.qualcomm.com/company/product-	O-QUA-SM73-121022/5793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25690		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5795
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22093		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5797
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM73-121022/5798
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM73-121022/5799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: sm7450_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5800
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5802
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5804
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22081		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5806
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5807
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5809
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5811
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5813
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5815
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5817
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM74-121022/5818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: sm8475p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5821
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5823
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5824
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5826
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5828
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5830
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5832
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5833
Time-of-check Time-of-	16-Sep-2022	7	Memory corruption in display due to	https://www.qualcomm.com/company/produc	O-QUA-SM84-121022/5834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5835
Product: sm8475_firmware					
Affected Version(s): -					
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	O-QUA-SM84-121022/5836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5837
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM84-121022/5838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5840
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5841
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5843
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5844
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5846
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5848
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SM84-121022/5849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5850
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SM84-121022/5852
Product: sw5100p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5854
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5856
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22081		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5858
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5860
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5862
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5864
Product: sw5100_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5865
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	O-QUA-SW51-121022/5866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5868
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5869
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-SW51-121022/5870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5871
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5873
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5875
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-SW51-121022/5876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcd9326_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5877
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5879
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCD9-121022/5880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5881
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5883
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5885
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5887
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5889
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption in display due to time-of-check time-	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/5890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	security/bulletins/september-2022-bulletin	
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5891
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcd9330_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5893
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCD9-121022/5894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5896
Product: wcd9335_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5897
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/5898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5899
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5902
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5904
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5906
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5908
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5910
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcd9340_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCD9-121022/5914
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5916
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5918
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5921
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5922
Product: wcd9341_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5924
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	ns/july-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5927
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5929
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5931
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5933
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5935
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5937
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5939
Product: wcd9360_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5940
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5942
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-WCD9-121022/5943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Product: wcd9370_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5945
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5946
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/5947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	security/bulletins/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5949
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5950
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5952
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5953
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to	https://www.qualcomm.com/company/produc	O-QUA-WCD9-121022/5954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5955
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5957
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5959
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/5960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5961
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5963
Product: wcd9371_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5965
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5967
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5969
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/5970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	security/bulletins/september-2022-bulletin	
Product: wcd9375_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5971
Buffer Copy without Checking	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/5972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5973
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5975
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5977
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5978
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5980
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5982
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5984
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5986
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5988
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5990
Product: wcd9380_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5992
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5993
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5995
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/5996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	ns/september-2022-bulletin	
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5997
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5998
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/5999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6000
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25693		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6002
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6004
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6006
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6008
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6010
Product: wcd9385_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6012
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6013
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCD9-121022/6014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6016
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6017
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6019
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6020
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to	https://www.qualcomm.com/company/produc	O-QUA-WCD9-121022/6021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6022
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6024
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6026
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	O-QUA-WCD9-121022/6027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6028
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCD9-121022/6030
Product: wcn3610_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22105		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6032
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6034
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6036
Product: wcn3615_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6040
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6042
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6044
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6046
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6048
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn3620_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6050
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6052
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6055
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6056
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while	https://www.qualcomm.com/company/product-	O-QUA-WCN3-121022/6057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	security/bulletins/september-2022-bulletin	
Product: wcn3660b_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6060
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6062
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6064
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6067
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6068
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	ns/september-2022-bulletin	
Product: wcn3660_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6070
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while	https://www.qualcomm.com/company/product-	O-QUA-WCN3-121022/6071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	security/bulletins/july-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22074		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6073
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6075
Product: wcn3680b_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6077
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6079
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6081
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6083
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6085
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6087
Product: wcn3680_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6089
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6091
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6093
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6095
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn3910_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6099
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6101
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6103
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6106
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6108
Product: wcn3950_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6109
Buffer Copy	16-Sep-2022	9.8	Memory corruption in video	https://www.qualcomm.com/c	O-QUA-WCN3-121022/6110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22066		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6112
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6114
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22091		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6116
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6118
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6120
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn3980_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6122
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6124
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6126
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6128
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6129
Integer Overflow or	16-Sep-2022	7.8	Possible integer overflow and memory	https://www.qualcomm.com/company/produc	O-QUA-WCN3-121022/6130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	t-security/bulletins/september-2022-bulletin	
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6132
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6134
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6136
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6138
Product: wcn3988_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25686		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6140
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6142
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6143
Integer Overflow	16-Sep-2022	7.8	Memory corruption in audio	https://www.qualcomm.com/c	O-QUA-WCN3-121022/6144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	ompany/product-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6145
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6147
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6149
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6152
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6153
Product: wcn3990_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6154
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6156
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6158
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6160
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6163
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6165
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6166
Product: wcn3991_firmware					
Affected Version(s): -					
Buffer Copy without	16-Sep-2022	9.8	Memory corruption in video module due to	https://www.qualcomm.com/company/produc	O-QUA-WCN3-121022/6167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	t-security/bulletins/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6168
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	ns/september-2022-bulletin	
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6171
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6172
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6174
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6176
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN3-121022/6177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6179
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6180
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6182
Product: wcn3998_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6184
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WCN3-121022/6186
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6188
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6190
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6192
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25669		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6194
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6196
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6198
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6200
Product: wcn3999_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6202
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6204
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6206
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN3-121022/6207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Product: wcn6740_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6208
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6210
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer	https://www.qualcomm.com/company/product-	O-QUA-WCN6-121022/6211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6212
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6214
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6216
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN6-121022/6217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6218
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN6-121022/6219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6220
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn6750_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6222
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6224
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6226
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6227
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6229
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6231
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6232
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6234
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-WCN6-121022/6235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6237
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6238
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN6-121022/6239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6240
Product: wcn6850_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN6-121022/6241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6242
Buffer Copy without Checking Size of Input ('Classic	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6244
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6246
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6247
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6249
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6251
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6254
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6256
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6257
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**		
Product: wcn6851_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6259
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6261
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6263
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6264
Use After Free	16-Sep-2022	7.8	Memory corruption in	https://www.qualcomm.com/c	O-QUA-WCN6-121022/6265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	ompany/product-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6266
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6268
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6270
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6272
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	O-QUA-WCN6-121022/6273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6274
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6276
Product: wcn6855_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6280
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6282
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6283
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6285
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6286
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	O-QUA-WCN6-121022/6287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6288
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	O-QUA-WCN6-121022/6289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6291
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6293
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6294
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-	https://www.qualcomm.com/company/produc	O-QUA-WCN6-121022/6295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	t-security/bulletins/september-2022-bulletin	
Product: wcn6856_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6296
Buffer Copy without Checking Size of	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WCN6-121022/6297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	ns/september-2022-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6298
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6300
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22081**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6302
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6303
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6305
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6307
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6309
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6311
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6313
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN6-121022/6314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: wcn7850_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6317
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6318
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	O-QUA-WCN7-121022/6319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6320
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6322
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6324
Time-of-check Time-of-use	16-Sep-2022	7	Memory corruption or temporary denial of service due to	https://www.qualcomm.com/company/product-	O-QUA-WCN7-121022/6325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6326
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6328
Product: wcn7851_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6330
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6332
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6334
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6335
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6337
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6338
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode	https://www.qualcomm.com/company/product-	O-QUA-WCN7-121022/6339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6340
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking	https://www.qualcomm.com/company/product-	O-QUA-WCN7-121022/6341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	security/bulletins/september-2022-bulletin	
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6343
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6345
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WCN7-121022/6346
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-	https://www.qualcomm.com/company/produc	O-QUA-WCN7-121022/6347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	t-security/bulletins/september-2022-bulletin	
Product: wsa8810_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6350
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WSA8-121022/6351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6352
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback	https://www.qualcomm.com/company/produc	O-QUA-WSA8-121022/6353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	t-security/bulletins/september-2022-bulletin	
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6354
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**		
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6356
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6358
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6360
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-	https://www.qualcomm.com/company/product-	O-QUA-WSA8-121022/6361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	security/bulletins/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6362
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-121022/6363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	ns/september-2022-bulletin	
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6364
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25654**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6366
Product: wsa8815_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	16-Sep-2022	9.8	Memory corruption in bluetooth due to integer overflow while processing HFP-UNIT profile in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-22105**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6368
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	26-Sep-2022	7.8	Memory corruption due to use after free issue in kernel while processing ION handles in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22058**	https://www.qualcomm.com/company/product-security/bulletins/july-2022-bulletin	O-QUA-WSA8-121022/6370
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**		
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6372
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22092		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6374
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6376
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6378
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**		
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6380
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6382
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25696		
Improper Input Validation	16-Sep-2022	6.7	Memory corruption in kernel due to improper input validation while processing ION commands in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables **CVE ID : CVE-2022-25654**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6384
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6385
Product: wsa8830_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6386
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6388
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6389
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-121022/6390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6391
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22089		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6393
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6394
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6396
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-22091**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6398
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**		
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6400
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6402
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6404
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25653		
Product: wsa8832_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6406
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables **CVE ID : CVE-2022-25688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25708**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6408
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6409
N/A	16-Sep-2022	7.8	Memory Corruption during	https://www.qualcomm.com/c	O-QUA-WSA8-121022/6410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**	ompany/product-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6411
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**		
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6413
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25656**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6415
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6416
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6418
Improper Validation of Array Index	16-Sep-2022	7.5	Information disclosure in WLAN due to improper validation of array index while parsing	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-121022/6419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25706**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6421
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6422
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race condition during map or unmap in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**		
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6424
Product: wsa8835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video module due to buffer overflow while processing WAV file in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25686**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in video due to buffer overflow while parsing ps video clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25688**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Memory corruption in WLAN due to buffer copy without checking size of input while parsing keys in Snapdragon Connectivity, Snapdragon Mobile	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25708		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption occurs while processing command received from HLOS due to improper length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-22066**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6428
N/A	16-Sep-2022	7.8	Memory Corruption during wma file playback due to integer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Music, Snapdragon Wearables **CVE ID : CVE-2022-22074**		
Out-of-bounds Read	16-Sep-2022	7.8	Memory corruption in audio module due to integer overflow in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22081**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6430
Integer Overflow or Wraparound	16-Sep-2022	7.8	Memory corruption in audio while playing record due to improper list handling in two threads in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22089**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6431
Use After Free	16-Sep-2022	7.8	Memory corruption in kernel due to use after free issue in Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22092**		
Use After Free	16-Sep-2022	7.8	Memory corruption in synx driver due to use-after-free condition in the synx driver due to accessing object handles without acquiring lock in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22095**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6433
Integer Overflow or Wraparound	16-Sep-2022	7.8	Possible integer overflow and memory corruption due to improper validation of buffer size sent to write to console when computing the payload size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25656		
Use After Free	16-Sep-2022	7.8	Memory corruption in graphics due to use-after-free while graphics profiling in Snapdragon Connectivity, Snapdragon Mobile **CVE ID : CVE-2022-25693**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6435
Incorrect Authorization	16-Sep-2022	7.5	Improper authorization of a replayed LTE security mode command can lead to a denial of service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-22091**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6436
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in video due to buffer over read while parsing MP4 clip in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25669**		
Out-of-bounds Read	16-Sep-2022	7.5	Denial of service in WLAN HOST due to buffer over read while unpacking frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2022-25670**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6438
Improper Validation	16-Sep-2022	7.5	Information disclosure in WLAN due to	https://www.qualcomm.com/company/produc	O-QUA-WSA8-121022/6439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			improper validation of array index while parsing crafted ANQP action frames in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music **CVE ID : CVE-2022-25690**	t-security/bulletins/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	7.5	Information disclosure in Bluetooth driver due to buffer over-read while reading l2cap length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25706		
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	Memory corruption or temporary denial of service due to improper handling of concurrent hypervisor operations to attach or detach IRQs from virtual interrupt sources in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22093**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6441
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Sep-2022	7	memory corruption in Kernel due to race condition while getting mapping reference in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile **CVE ID : CVE-2022-22094**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6442
Time-of-check Time-of-use (TOCTOU)	16-Sep-2022	7	Memory corruption in display due to time-of-check time-of-use race	https://www.qualcomm.com/company/product-security/bulleti	O-QUA-WSA8-121022/6443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			condition during map or unmap in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25696**	ns/september-2022-bulletin	
Out-of-bounds Read	16-Sep-2022	5.5	Information disclosure in video due to buffer over-read while processing avi file in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2022-25653**	https://www.qualcomm.com/company/product-security/bulletins/september-2022-bulletin	O-QUA-WSA8-121022/6444
Vendor: Realtek					
Product: rtl8195am_firmware					
Affected Version(s): * Up to (excluding) 2022-06-20					
N/A	27-Sep-2022	7.5	On Realtek RTL8195AM devices before 284241d70308ff2519e40afd7b284ba	https://www.realtek.com/en	O-REA-RTL8-121022/6445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			892c730a3, the timer task can be locked when there are frequent and continuous Wi-Fi connection failures for the Soft AP mode. **CVE ID : CVE-2022-34326**		
Vendor: Samsung					
Product: tizenrt					
Affected Version(s): 2.0					
Use After Free	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). createDB in security/provisioning/src/provisioningdatabasemanager.c has a missing sqlite3_free after sqlite3_exec, leading to a denial of service. **CVE ID : CVE-2022-40278**	N/A	O-SAM-TIZE-121022/6446
Unchecked Return Value	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). l2_packet_receive_timeout in wpa_supplicant/src/l2_packet/l2_packet_pcap.c has a missing check on the return value of pcap_dispatch,	N/A	O-SAM-TIZE-121022/6447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to a denial of service (malfunction). **CVE ID : CVE-2022-40279**		
Affected Version(s): 3.0					
Use After Free	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). createDB in security/provisioning/src/provisioningdatabasemanager.c has a missing sqlite3_free after sqlite3_exec, leading to a denial of service. **CVE ID : CVE-2022-40278**	N/A	O-SAM-TIZE-121022/6448
Unchecked Return Value	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). l2_packet_receive_timeout in wpa_supplicant/src/l2_packet/l2_packet_pcap.c has a missing check on the return value of pcap_dispatch, leading to a denial of service (malfunction). **CVE ID : CVE-2022-40279**	N/A	O-SAM-TIZE-121022/6449
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). createDB in security/provisioning/src/provisioningdatabasemanager.c has a missing sqlite3_free after sqlite3_exec, leading to a denial of service. **CVE ID : CVE-2022-40278**	N/A	O-SAM-TIZE-121022/6450
Unchecked Return Value	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). l2_packet_receive_timeout in wpa_supplicant/src/l2_packet/l2_packet_pcap.c has a missing check on the return value of pcap_dispatch, leading to a denial of service (malfunction). **CVE ID : CVE-2022-40279**	N/A	O-SAM-TIZE-121022/6451
Affected Version(s): 1.1					
Use After Free	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). createDB in security/provisioni	N/A	O-SAM-TIZE-121022/6452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ng/src/provisioningdatabasemanager.c has a missing sqlite3_free after sqlite3_exec, leading to a denial of service. **CVE ID : CVE-2022-40278**		
Unchecked Return Value	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). l2_packet_receive_timeout in wpa_supplicant/src/l2_packet/l2_packet_pcap.c has a missing check on the return value of pcap_dispatch, leading to a denial of service (malfunction). **CVE ID : CVE-2022-40279**	N/A	O-SAM-TIZE-121022/6453
Affected Version(s): 3.1					
Use After Free	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). createDB in security/provisioning/src/provisioningdatabasemanager.c has a missing sqlite3_free after sqlite3_exec, leading to a denial of service.	N/A	O-SAM-TIZE-121022/6454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40278		
Unchecked Return Value	29-Sep-2022	7.5	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). l2_packet_receive_timeout in wpa_supplicant/src/l2_packet/l2_packet_pcap.c has a missing check on the return value of pcap_dispatch, leading to a denial of service (malfunction). **CVE ID : CVE-2022-40279**	N/A	O-SAM-TIZE-121022/6455
Vendor: Sony					
Product: playstation_4_firmware					
Affected Version(s): -					
Out-of-bounds Write	28-Sep-2022	6.8	A vulnerability was found in Sony PS4 and PS5. It has been classified as critical. This affects the function UVFAT_readupcase table of the component exFAT Handler. The manipulation of the argument dataLength leads to heap-based buffer overflow. It is possible to launch the attack on the physical device. It is recommended to	N/A	O-SON-PLAY-121022/6456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. The associated identifier of this vulnerability is VDB-209679. **CVE ID : CVE-2022-3349**		
Product: playstation_5_firmware					
Affected Version(s): -					
Out-of-bounds Write	28-Sep-2022	6.8	A vulnerability was found in Sony PS4 and PS5. It has been classified as critical. This affects the function UVFAT_readupcase table of the component exFAT Handler. The manipulation of the argument dataLength leads to heap-based buffer overflow. It is possible to launch the attack on the physical device. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-209679. **CVE ID : CVE-2022-3349**	N/A	O-SON-PLAY-121022/6457
Vendor: tacitine					
Product: en6200-prime_quad-100_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 19.1.1 Up to (excluding) 22.21.2					
Improper Control of Generation of Code ('Code Injection')	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper control of code generation in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to execute arbitrary commands on the targeted device. **CVE ID : CVE-2022-40628**	https://tacitine.com/newdownload/CVE-2022-40628.pdf	O-TAC-EN62-121022/6458
Session Fixation	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and	https://tacitine.com/newdownload/CVE-2022-40630.pdf	O-TAC-EN62-121022/6459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper session management in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to perform session fixation on the targeted device. **CVE ID : CVE-2022-40630**		
N/A	23-Sep-2022	7.5	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to insecure design in the Tacitine Firewall	https://tacitine.com/newdownload/CVE-2022-40629.pdf	O-TAC-EN62-121022/6460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to view sensitive information on the targeted device. **CVE ID : CVE-2022-40629**		
Product: en6200-prime_quad-35_firmware					
Affected Version(s): From (including) 19.1.1 Up to (excluding) 22.21.2					
Improper Control of Generation of Code ('Code Injection')	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper control of code generation in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker	https://tacitine.com/newdownload/CVE-2022-40628.pdf	O-TAC-EN62-121022/6461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to execute arbitrary commands on the targeted device. **CVE ID : CVE-2022-40628**		
Session Fixation	23-Sep-2022	9.8	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to improper session management in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful	https://tacitine.com/newdownload/CVE-2022-40630.pdf	O-TAC-EN62-121022/6462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability could allow an unauthenticated remote attacker to perform session fixation on the targeted device. **CVE ID : CVE-2022-40630**		
N/A	23-Sep-2022	7.5	This vulnerability exists in Tacitine Firewall, all versions of EN6200-PRIME QUAD-35 and EN6200-PRIME QUAD-100 between 19.1.1 to 22.20.1 (inclusive), due to insecure design in the Tacitine Firewall web-based management interface. An unauthenticated remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted device. Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to view sensitive information on the targeted device.	https://tacitine.com/newdownload/CVE-2022-40629.pdf	O-TAC-EN62-121022/6463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40629		
Vendor: Tenda					
Product: ac15_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 V15.03.05.19 contained a stack overflow via the function fromAddressNat. **CVE ID : CVE-2022-40851**	N/A	O-TEN-AC15-121022/6464
Product: ac18_firmware					
Affected Version(s): 15.03.05.19\\(6318\\)					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC18 router contained a stack overflow vulnerability in /goform/fast_setting_wifi_set **CVE ID : CVE-2022-40854**	N/A	O-TEN-AC18-121022/6465
Out-of-bounds Write	23-Sep-2022	7.2	Tenda AC18 router V15.03.05.19 contains a stack overflow vulnerability in the formSetQosBand->FUN_0007db78 function with the request /goform/SetNetControlList/ **CVE ID : CVE-2022-40861**	N/A	O-TEN-AC18-121022/6466
Product: ac21_firmware					
Affected Version(s): 16.03.08.15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: formSetVirtualSer. **CVE ID : CVE-2022-40067**	N/A	O-TEN-AC21-121022/6467
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: formSetQosBand. **CVE ID : CVE-2022-40068**	N/A	O-TEN-AC21-121022/6468
Out-of-bounds Write	19-Sep-2022	7.5	]Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: fromSetSysTime. **CVE ID : CVE-2022-40069**	N/A	O-TEN-AC21-121022/6469
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via bin/httpd, function: formSetFirewallCfg . **CVE ID : CVE-2022-40070**	N/A	O-TEN-AC21-121022/6470
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via	N/A	O-TEN-AC21-121022/6471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/bin/httpd, formSetDeviceName. **CVE ID : CVE-2022-40071**		
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: setSmartPowerManagement. **CVE ID : CVE-2022-40072**	N/A	O-TEN-AC21-121022/6472
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, saveParentControlInfo. **CVE ID : CVE-2022-40073**	N/A	O-TEN-AC21-121022/6473
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, setSchedWifi. **CVE ID : CVE-2022-40074**	N/A	O-TEN-AC21-121022/6474
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V 16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, form_fast_setting_wifi_set. **CVE ID : CVE-2022-40075**	N/A	O-TEN-AC21-121022/6475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Sep-2022	7.5	Tenda AC21 V16.03.08.15 is vulnerable to Buffer Overflow via /bin/httpd, function: fromSetWifiGusetBasic. **CVE ID : CVE-2022-40076**	N/A	O-TEN-AC21-121022/6476
Product: i9_firmware					
Affected Version(s): 1.0.0.8\\(3828\\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Sep-2022	9.8	Tenda i9 v1.0.0.8(3828) was discovered to contain a command injection vulnerability via the FormexeCommand function. **CVE ID : CVE-2022-40100**	N/A	O-TEN-I9_F-121022/6477
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formWifiMacFilterSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40101**	N/A	O-TEN-I9_F-121022/6478
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer	N/A	O-TEN-I9_F-121022/6479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the formwrlSSIDset function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40102**		
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formwrlSSIDget function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40104**	N/A	O-TEN-I9_F-121022/6480
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formWifiMacFilterGet function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40105**	N/A	O-TEN-I9_F-121022/6481
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer	N/A	O-TEN-I9_F-121022/6482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the set_local_time function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40106**		
Out-of-bounds Write	23-Sep-2022	7.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formexeCommand function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40107**	N/A	O-TEN-I9_F-121022/6483
Out-of-bounds Write	23-Sep-2022	5.5	Tenda i9 v1.0.0.8(3828) was discovered to contain a buffer overflow via the formSetAutoPing function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted string. **CVE ID : CVE-2022-40103**	N/A	O-TEN-I9_F-121022/6484
Product: rx9_pro_firmware					
Affected Version(s): 22.03.02.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Tenda RX9_Pro V22.03.02.10 is vulnerable to Buffer Overflow via httpd/setMacFilterCfg. **CVE ID : CVE-2022-38829**	N/A	O-TEN-RX9_-121022/6485
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Tenda RX9_Pro V22.03.02.10 is vulnerable to Buffer Overflow via httpd/setIPv6Status. **CVE ID : CVE-2022-38830**	N/A	O-TEN-RX9_-121022/6486
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	Tenda RX9_Pro V22.03.02.10 is vulnerable to Buffer Overflow via httpd/SetNetControlList **CVE ID : CVE-2022-38831**	N/A	O-TEN-RX9_-121022/6487
Product: tx3_firmware					
Affected Version(s): 16.03.13.11					
Out-of-bounds Write	28-Sep-2022	9.8	Tenda TX3 US_TX3V1.0br_V16.03.13.11 is vulnerable to stack overflow via compare_parentcontrol_time. **CVE ID : CVE-2022-40942**	N/A	O-TEN-TX3_-121022/6488
Product: w20e_firmware					
Affected Version(s): 15.11.0.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 contains a stack overflow in the function formSetPortMapping with post request 'goform/setPortMapping/'. This vulnerability allows attackers to cause a Denial of Service (DoS) or Remote Code Execution (RCE) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters. **CVE ID : CVE-2022-40855**	N/A	O-TEN-W20E-121022/6489
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formSetDebugCfg with request /goform/setDebugCfg/ **CVE ID : CVE-2022-40866**	N/A	O-TEN-W20E-121022/6490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formIPMacBindDel with the request /goform/delIpMacBind/ **CVE ID : CVE-2022-40867**	N/A	O-TEN-W20E-121022/6491
Out-of-bounds Write	23-Sep-2022	9.8	Tenda W20E router V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC) contains a stack overflow vulnerability in the function formDelDhcpRule with the request /goform/delDhcpRules/ **CVE ID : CVE-2022-40868**	N/A	O-TEN-W20E-121022/6492
Vendor: Tendacn					
Product: ac15_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 router V15.03.05.19 contains a stack overflow via the list parameter at /goform/fast_setting_wifi_set	N/A	O-TEN-AC15-121022/6493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-40853		
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 router V15.03.05.19 contains a stack overflow vulnerability in the function formSetQosBand->FUN_0007dd20 with request /goform/SetNetControlList **CVE ID : CVE-2022-40860**	N/A	O-TEN-AC15-121022/6494
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 router V15.03.05.19 contains stack overflow vulnerability in the function fromNatStaticSetting with the request /goform/NatStaticSetting **CVE ID : CVE-2022-40862**	N/A	O-TEN-AC15-121022/6495
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function setSmartPowerManagement with the request /goform/PowerSaveSet **CVE ID : CVE-2022-40864**	N/A	O-TEN-AC15-121022/6496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain heap overflow vulnerabilities in the function setSchedWifi with the request /goform/openSchedWifi/ **CVE ID : CVE-2022-40865**	N/A	O-TEN-AC15-121022/6497
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function fromDhcpListClient with a combined parameter "list*" ("%s%d","list"). **CVE ID : CVE-2022-40869**	N/A	O-TEN-AC15-121022/6498
Product: ac18_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 router V15.03.05.19 contains stack overflow vulnerability in the function fromNatStaticSetting with the request /goform/NatStaticSetting **CVE ID : CVE-2022-40862**	N/A	O-TEN-AC18-121022/6499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function setSmartPowerManagement with the request /goform/PowerSaveSet **CVE ID : CVE-2022-40864**	N/A	O-TEN-AC18-121022/6500
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain heap overflow vulnerabilities in the function setSchedWifi with the request /goform/openSchedWifi/ **CVE ID : CVE-2022-40865**	N/A	O-TEN-AC18-121022/6501
Out-of-bounds Write	23-Sep-2022	9.8	Tenda AC15 and AC18 routers V15.03.05.19 contain stack overflow vulnerabilities in the function fromDhcpListClient with a combined parameter "list*" ("%s%d","list"). **CVE ID : CVE-2022-40869**	N/A	O-TEN-AC18-121022/6502
Vendor: Tesla					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: model_3_firmware					
Affected Version(s): 11.0					
Authentication Bypass by Spoofing	16-Sep-2022	5.3	Tesla Model 3 V11.0(2022.4.5.1 6b701552d7a6) Tesla mobile app v4.23 is vulnerable to Authentication Bypass by spoofing. Tesla Model 3's Phone Key authentication is vulnerable to Man-in-the-middle attacks in the BLE channel. It allows attackers to open a door and drive the car away by leveraging access to a legitimate Phone Key. **CVE ID : CVE-2022-37709**	N/A	O-TES-MODE-121022/6503
Vendor: toaruos					
Product: toaruos					
Affected Version(s): 2.0.1					
Out-of-bounds Write	27-Sep-2022	7.8	readelf in ToaruOS 2.0.1 has a global overflow allowing RCE when parsing a crafted ELF file. **CVE ID : CVE-2022-38932**	https://github.com/klange/toaruos/issues/243	O-TOA-TOAR-121022/6504
Out-of-bounds Read	28-Sep-2022	3.3	readelf in ToaruOS 2.0.1 has some arbitrary address read vulnerabilities when parsing a crafted ELF file.	https://github.com/klange/toaruos/issues/244	O-TOA-TOAR-121022/6505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38934		
Vendor: totolink					
Product: t6_firmware					
Affected Version(s): 4.1.5cu.709_b20210518					
Use of Hard-coded Credentials	16-Sep-2022	9.8	In TOTOLINK T6 V4.1.5cu.709_B20210518, there is a hard coded password for root in /etc/shadow.sample. **CVE ID : CVE-2022-38823**	N/A	O-TOT-T6_F-121022/6506
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Sep-2022	9.8	In TOTOLINK T6 V4.1.5cu.709_B20210518, there is an execute arbitrary command in cstecgi.cgi. **CVE ID : CVE-2022-38826**	N/A	O-TOT-T6_F-121022/6507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Sep-2022	9.8	TOTOLINK T6 V4.1.5cu.709_B20210518 is vulnerable to Buffer Overflow via cstecgi.cgi **CVE ID : CVE-2022-38827**	N/A	O-TOT-T6_F-121022/6508
Improper Neutralization of Special Elements used in a Command	16-Sep-2022	9.8	TOTOLINK T6 V4.1.5cu.709_B20210518 is vulnerable to command injection via cstecgi.cgi	N/A	O-TOT-T6_F-121022/6509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			**CVE ID : CVE-2022-38828**		
Vendor: Tp-link					
Product: archer_ax10_v1_firmware					
Affected Version(s): 1.3.1					
Improper Control of Generation of Code ('Code Injection')	28-Sep-2022	8.8	TP Link Archer AX10 V1 Firmware Version 1.3.1 Build 20220401 Rel. 57450(5553) was discovered to allow authenticated attackers to execute arbitrary code via a crafted backup file. **CVE ID : CVE-2022-40486**	N/A	O-TP--ARCH-121022/6510
Vendor: ZTE					
Product: zxa10_b700v7_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6511
Product: zxa10_b710c-a12_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6512
Product: zxa10_b710s2-a19_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6513
Product: zxa10_b766v2_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB	https://support.zte.com.cn/support/news/LoopholeInfoDetail.	O-ZTE-ZXA1-121022/6514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	aspx?newsId=1026224	
Product: zxa10_b76hv3_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6515
Product: zxa10_b800v2_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**		
Product: zxa10_b836ct-a15_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6517
Product: zxa10_b860av2.1_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system.	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23144		
Product: zxa10_b860h_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6519
Product: zxa10_b866v2-h_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6520
Product: zxa10_b866v5-w10_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6521
Product: zxa10_b960gv1_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6522
Product: zxa10_s100v_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to	https://support.zte.com.cn/support/news/LoopholeInfoDetail.	O-ZTE-ZXA1-121022/6523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	aspx?newsId=1026224	
Product: zxa10_s200a_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6524
Product: zxa10_s200t_firmware					
Affected Version(s): * Up to (including) 2.01.02.01					
Improper Link Resolution Before File Access ('Link Following')	23-Sep-2022	9.1	There is a broken access control vulnerability in ZTE ZXvSTB product. Due to improper permission control, attackers could use this vulnerability to delete the	https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1026224	O-ZTE-ZXA1-121022/6525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default application type, which affects normal use of system. **CVE ID : CVE-2022-23144**		
Vendor: Zyxel					
Product: gs1900-10hp_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aazi.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6526
Product: gs1900-16_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aahj.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the	https://www.zyxel.com/global/en/support/security-	O-ZYX-GS19-121022/6527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	
Product: gs1900-24ep_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(abto.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**		
Product: gs1900-24e_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aahk.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6529
Product: gs1900-24hpv2_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(abtp.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the	https://www.zyxel.com/global/en/support/security-	O-ZYX-GS19-121022/6530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	
Product: gs1900-24_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aahl.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**		
Product: gs1900-48hpv2_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(abtq.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6532
Product: gs1900-48_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aahn.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the	https://www.zyxel.com/global/en/support/security-	O-ZYX-GS19-121022/6533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	
Product: gs1900-8hp_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aahi.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**		
Product: gs1900-8_firmware					
Affected Version(s): * Up to (excluding) 2.70\\(aahh.3\\)c0					
Insufficient Entropy	20-Sep-2022	5.9	An insufficient entropy vulnerability caused by the improper use of randomness sources with low entropy for RSA key pair generation was found in Zyxel GS1900 series firmware versions prior to V2.70. This vulnerability could allow an unauthenticated attacker to retrieve a private key by factoring the RSA modulus N in the certificate of the web administration interface. **CVE ID : CVE-2022-34746**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-insufficient-entropy-vulnerability-of-gs1900-series-switches	O-ZYX-GS19-121022/6535