National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Mar 2023 Vol. 10 No. 05

Table of Content

Vendor	Product	Page Number
yoga_class_registration_system_project	yoga_class_registration_system	584
Zohocorp	manageengine_assetexplorer	585
	manageengine_servicedesk_plus	586
	manageengine_servicedesk_plus_msp	588
	manageengine_supportcenter_plus	589
\@nubosoftware\/node-static_project	\@nubosoftware\/node-static	590
Hardware		
akuvox	e11	591
apsystems	energy_communication_unit	594
Arubanetworks	7010	595
	7030	600
	7205	605
	7210	610
	7220	615
	7240xm	619
	7280	624
	9004	629
	9004-lte	634
	9012	639
	mc-va-10	644
	mc-va-1k	649
	mc-va-250	654
	mc-va-50	659
	mcr-hw-10k	664
	mcr-hw-1k	669
	mcr-hw-5k	674
	mcr-va-10k	679
	mcr-va-1k	683
	mcr-va-50	688
	mcr-va-500	693
	mcr-va-5k	698

Vendor	Product	Page Number
Draytek	virgor2866ac	827
	virgor2866ax	828
	virgor2866l	829
	virgor2866lac	830
	virgor2866vac	831
	virgor2915	832
	virgor2915ac	832
	virgor2925	833
	virgor2925ac	834
	virgor2925fn	835
	virgor2925l	836
	virgor2925ln	836
	virgor2925n	837
	virgor2925n-plus	838
	virgor2925vac	839
	virgor2925vn-plus	840
	virgor2926	841
	virgor2926ac	841
	virgor2926l	842
	virgor2926lac	843
	virgor2926ln	844
	virgor2926n	845
	virgor2926vac	845
	virgor2927	846
	virgor2927ac	847
	virgor2927ax	848
	virgor2927f	849
	virgor2927l	850
	virgor2927lac	850
	virgor2927vac	851
	virgor2952	852
	virgor2952p	853

Vendor	Product	Page Number
mediatek	mt6877	991
	mt6879	998
	mt6883	1008
	mt6885	1014
	mt6889	1023
	mt6891	1029
	mt6893	1033
	mt6895	1041
	mt6983	1051
	mt6985	1061
	mt8167	1062
	mt8167s	1064
	mt8168	1065
	mt8173	1067
	mt8175	1068
	mt8185	1068
	mt8195z	1069
	mt8321	1069
	mt8362a	1074
	mt8365	1075
	mt8385	1075
	mt8532	1076
	mt8666	1077
	mt8667	1079
	mt8675	1080
	mt8765	1082
	mt8766	1088
	mt8768	1093
	mt8781	1099
	mt8785	1106
	mt8786	1106
	mt8788	1112

Vendor	Product	Page Number
mediatek	mt8789	1118
	mt8791	1124
	mt8791t	1128
	mt8797	1135
Mitsubishielectric	fx5-enet	1143
	fx5-enet\/ip	1144
	fx5s-30mr\/es	1145
	fx5s-30mt\/es	1145
	fx5s-30mt\/ess	1146
	fx5s-40mr\/es	1147
	fx5s-40mt\/es	1147
	fx5s-40mt\/ess	1148
	fx5s-60mr\/es	1149
	fx5s-60mt\/es	1149
	fx5s-60mt\/ess	1150
	fx5s-80mr\/es	1151
	fx5s-80mt\/es	1151
	fx5s-80mt\/ess	1152
	fx5uc-32mr\/ds-ts	1153
	fx5uc-32mt\/d	1153
	fx5uc-32mt\/ds-ts	1154
	fx5uc-32mt\/dss	1155
	fx5uc-32mt\/dss-ts	1155
	fx5uc-64mt\/d	1156
	fx5uc-64mt\/dss	1157
	fx5uc-96mt\/d	1157
	fx5uc-96mt\/dss	1158
	fx5uj-24mr\/es	1159
	fx5uj-24mr\/es-a	1159
	fx5uj-24mt\/es	1160
	fx5uj-24mt\/es-a	1161
	fx5uj-24mt\/ess	1161

Vendor	Product	Page Number
Mitsubishielectric	fx5uj-40mr\/es	1162
	fx5uj-40mr\/es-a	1163
	fx5uj-40mt\/es	1163
	fx5uj-40mt\/es-a	1164
	fx5uj-40mt\/ess	1165
	fx5uj-60mr\/es	1165
	fx5uj-60mr\/es-a	1166
	fx5uj-60mt\/es	1167
	fx5uj-60mt\/es-a	1167
	fx5uj-60mt\/ess	1168
Moxa	uc-2101-lx	1169
	uc-2102-lx	1169
	uc-2102-t-lx	1170
	uc-2104-lx	1170
	uc-2111-lx	1171
	uc-2112-lx	1172
	uc-2114-t-lx	1172
	uc-2116-t-lx	1173
	uc-3101-t-ap-lx	1173
	uc-3101-t-eu-lx	1174
	uc-3101-t-us-lx	1174
	uc-3111-t-ap-lx	1175
	uc-3111-t-ap-lx-nw	1175
	uc-3111-t-eu-lx	1176
	uc-3111-t-eu-lx-nw	1177
	uc-3111-t-us-lx	1177
	uc-3111-t-us-lx-nw	1178
	uc-3121-t-ap-lx	1178
	uc-3121-t-eu-lx	1179
	uc-3121-t-us-lx	1179
	uc-5101-lx	1180
	uc-5101-t-lx	1180

Vendor	Product	Page Number
Moxa	uc-5102-lx	1181
	uc-5102-t-lx	1182
	uc-5111-lx	1182
	uc-5111-t-lx	1183
	uc-5112-lx	1183
	uc-5112-t-lx	1184
	uc-8112-lx	1184
	uc-8112-me-t-lx	1185
	uc-8112-me-t-lx1	1185
	uc-8112a-me-t-lx	1186
	uc-8131-lx	1187
	uc-8132-lx	1187
	uc-8162-lx	1188
	uc-8210-t-lx-s	1188
	uc-8220-t-lx	1189
	uc-8220-t-lx-ap-s	1189
	uc-8220-t-lx-eu-s	1190
	uc-8220-t-lx-s	1190
	uc-8220-t-lx-us-s	1191
	uc-8410a-lx	1192
	uc-8410a-nw-lx	1192
	uc-8410a-nw-t-lx	1193
	uc-8410a-t-lx	1193
	uc-8540-lx	1194
	uc-8540-t-ct-lx	1194
	uc-8540-t-lx	1195
	uc-8580-lx	1195
	uc-8580-q-lx	1196
	uc-8580-t-ct-lx	1197
	uc-8580-t-ct-q-lx	1197
	uc-8580-t-lx	1198
	uc-8580-t-q-lx	1198

Vendor	Product	Page Number
Sonicwall	nsa_9450	1237
	nsa_9650	1237
	nssp12400	1238
	nssp12800	1238
	nssp_10700	1238
	nssp_11700	1239
	nssp_13700	1240
	nssp_15700	1240
	nsv_10	1241
	nsv_100	1241
	nsv_1600	1242
	nsv_200	1243
	nsv_25	1243
	nsv_270	1244
	nsv_300	1245
	nsv_400	1245
	nsv_470	1246
	nsv_50	1246
	nsv_800	1247
	nsv_870	1248
	sm10200	1248
	sm10400	1249
	sm10800	1249
	sm9200	1249
	sm9400	1250
	sm9600	1250
	sm9800	1250
	sohow	1250
	soho_250	1251
	soho_250w	1251
	tz270	1251
	tz270w	1252

Vendor	Product	Page Number
Draytek	vigor166_firmware	1353
	vigor2133ac_firmware	1353
	vigor2133fvac_firmware	1354
	vigor2133n_firmware	1355
	vigor2133vac_firmware	1356
	vigor2133_firmware	1357
	vigor2135ac_firmware	1358
	vigor2135ax_firmware	1358
	vigor2135fvac_firmware	1359
	vigor2135vac_firmware	1360
	vigor2135_firmware	1361
	vigor2762ac_firmware	1362
	vigor2762n_firmware	1362
	vigor2762vac_firmware	1363
	vigor2762_firmware	1364
	vigor2763ac_firmware	1365
	vigor2763_firmware	1366
	vigor2765ac_firmware	1367
	vigor2765ax_firmware	1367
	vigor2765va_firmware	1368
	vigor2765_firmware	1369
	vigor2766ac_firmware	1370
	vigor2766ax_firmware	1371
	vigor2766vac_firmware	1372
	vigor2766_firmware	1372
	vigor2832n_firmware	1373
	vigor2832_firmware	1374
	vigor2860ac_firmware	1375
	vigor2860ln_firmware	1376
	vigor2860l_firmware	1376
	vigor2860n-plus_firmware	1377
	vigor2860n_firmware	1378

Vendor	Product	Page Number
Draytek	vigor2860vac_firmware	1379
	vigor2860vn-plus_firmware	1380
	vigor2860_firmware	1381
	vigor2960_firmware	1381
	vigornic_132_firmware	1382
	vigor_2960_firmware	1383
	virgor1000b_firmware	1384
	virgor2862ac_firmware	1385
	virgor2862bn_firmware	1385
	virgor2862b_firmware	1386
	virgor2862lac_firmware	1387
	virgor2862ln_firmware	1388
	virgor2862l_firmware	1389
	virgor2862n_firmware	1390
	virgor2862vac_firmware	1390
	virgor2862_firmware	1391
	virgor2865ac_firmware	1392
	virgor2865ax_firmware	1393
	virgor2865lac_firmware	1394
	virgor2865l_firmware	1394
	virgor2865vac_firmware	1395
	virgor2865_firmware	1396
	virgor2866ac_firmware	1397
	virgor2866ax_firmware	1398
	virgor2866lac_firmware	1399
	virgor2866l_firmware	1399
	virgor2866vac_firmware	1400
	virgor2866_firmware	1401
	virgor2915ac_firmware	1402
	virgor2915_firmware	1403
	virgor2925ac_firmware	1404
	virgor2925fn_firmware	1404

Vendor	Product	Page Number
Draytek	virgor2925ln_firmware	1405
	virgor2925l_firmware	1406
	virgor2925n-plus_firmware	1407
	virgor2925n_firmware	1408
	virgor2925vac_firmware	1408
	virgor2925vn-plus_firmware	1409
	virgor2925_firmware	1410
	virgor2926ac_firmware	1411
	virgor2926lac_firmware	1412
	virgor2926ln_firmware	1413
	virgor2926l_firmware	1413
	virgor2926n_firmware	1414
	virgor2926vac_firmware	1415
	virgor2926_firmware	1416
	virgor2927ac_firmware	1417
	virgor2927ax_firmware	1418
	virgor2927f_firmware	1418
	virgor2927lac_firmware	1419
	virgor2927l_firmware	1420
	virgor2927vac_firmware	1421
	virgor2927_firmware	1422
	virgor2952p_firmware	1422
	virgor2952_firmware	1423
	virgor2962p_firmware	1424
	virgor2962_firmware	1425
	virgor3220_firmware	1426
	virgor3910_firmware	1427
Fedoraproject	fedora	1427
gigamon	gigavue-os	1428
Google	android	1428
	linux_and_chrome_os	1459
heimgardtechnologies	eagle_1200ac_firmware	1459

Vendor	Product	Page Number
HP	hp-ux	1465
IBM	aix	1465
	z\/os	1466
kylinos	kylin_os	1466
Linux	linux_kernel	1468
Microsoft	windows	1471
	windows_10	1477
	windows_10_1507	1479
	windows_10_1607	1485
	windows_10_1809	1494
	windows_10_20h2	1503
	windows_10_21h2	1512
	windows_10_22h2	1521
	windows_11_21h2	1530
	windows_11_22h2	1540
	windows_server_2008	1549
	windows_server_2012	1555
	windows_server_2016	1571
	windows_server_2019	1580
	windows_server_2022	1589
Mitsubishielectric	fx5-enet\/ip_firmware	1599
	fx5-enet_firmware	1600
	fx5s-30mr\/es_firmware	1600
	fx5s-30mt\/ess_firmware	1601
	fx5s-30mt\/es_firmware	1602
	fx5s-40mr\/es_firmware	1602
	fx5s-40mt\/ess_firmware	1603
	fx5s-40mt\/es_firmware	1604
	fx5s-60mr\/es_firmware	1604
	fx5s-60mt\/ess_firmware	1605
	fx5s-60mt\/es_firmware	1606
	fx5s-80mr\/es_firmware	1606

Vendor	Product	Page Number
Mitsubishielectric	fx5s-80mt\/ess_firmware	1607
	fx5s-80mt\/es_firmware	1608
	fx5uc-32mr\/ds-ts_firmware	1608
	fx5uc-32mt\/ds-ts_firmware	1609
	fx5uc-32mt\/dss-ts_firmware	1610
	fx5uc-32mt\/dss_firmware	1610
	fx5uc-32mt\/d_firmware	1611
	fx5uc-64mt\/dss_firmware	1612
	fx5uc-64mt\/d_firmware	1612
	fx5uc-96mt\/dss_firmware	1613
	fx5uc-96mt\/d_firmware	1614
	fx5uj-24mr\/es-a_firmware	1614
	fx5uj-24mr\/es_firmware	1615
	fx5uj-24mt\/es-a_firmware	1616
	fx5uj-24mt\/ess_firmware	1616
	fx5uj-24mt\/es_firmware	1617
	fx5uj-40mr\/es-a_firmware	1618
	fx5uj-40mr\/es_firmware	1618
	fx5uj-40mt\/es-a_firmware	1619
	fx5uj-40mt\/ess_firmware	1620
	fx5uj-40mt\/es_firmware	1620
	fx5uj-60mr\/es-a_firmware	1621
	fx5uj-60mr\/es_firmware	1622
	fx5uj-60mt\/es-a_firmware	1622
	fx5uj-60mt\/ess_firmware	1623
	fx5uj-60mt\/es_firmware	1624
Moxa	uc-2101-lx_firmware	1624
	uc-2102-lx_firmware	1625
	uc-2102-t-lx_firmware	1626
	uc-2104-lx_firmware	1626
	uc-2111-lx_firmware	1627
	uc-2112-lx_firmware	1627

Vendor	Product	Page Number
Moxa	uc-2114-t-lx_firmware	1628
	uc-2116-t-lx_firmware	1629
	uc-3101-t-ap-lx_firmware	1629
	uc-3101-t-eu-lx_firmware	1630
	uc-3101-t-us-lx_firmware	1630
	uc-3111-t-ap-lx-nw_firmware	1631
	uc-3111-t-ap-lx_firmware	1632
	uc-3111-t-eu-lx-nw_firmware	1632
	uc-3111-t-eu-lx_firmware	1633
	uc-3111-t-us-lx-nw_firmware	1633
	uc-3111-t-us-lx_firmware	1634
	uc-3121-t-ap-lx_firmware	1634
	uc-3121-t-eu-lx_firmware	1635
	uc-3121-t-us-lx_firmware	1636
	uc-5101-lx_firmware	1636
	uc-5101-t-lx_firmware	1637
	uc-5102-lx_firmware	1637
	uc-5102-t-lx_firmware	1638
	uc-5111-lx_firmware	1638
	uc-5111-t-lx_firmware	1639
	uc-5112-lx_firmware	1639
	uc-5112-t-lx_firmware	1640
	uc-8112-lx_firmware	1641
	uc-8112-me-t-lx1_firmware	1641
	uc-8112-me-t-lx_firmware	1642
	uc-8112a-me-t-lx_firmware	1642
	uc-8131-lx_firmware	1643
	uc-8132-lx_firmware	1643
	uc-8162-lx_firmware	1644
	uc-8210-t-lx-s_firmware	1644
	uc-8220-t-lx-ap-s_firmware	1645
	uc-8220-t-lx-eu-s_firmware	1646

Vendor	Product	Page Number
sauter-controls	nova_106_eyk300f001_firmware	1687
	nova_220_eyk220f001_firmware	1687
	nova_230_eyk230f001_firmware	1688
Sonicwall	sonicos	1689
Suse	linux_enterprise_server	1691
Tenda	ax3_firmware	1691
	w15e_firmware	1692
totolink	a7100ru_firmware	1694
Tp-link	archer_ax21_firmware	1695
yoctoproject	yocto	1695

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: map_builder_for_google_maps					
Affected Version(s): * Up to (excluding) 1.0.73					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	9.8	The 10Web Map Builder for Google Maps WordPress plugin before 1.0.73 does not properly sanitise and escape some parameters before using them in an SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection **CVE ID : CVE-2023-0037**	N/A	A-10W-MAP_-280323/1
Vendor: 115cms					
Product: 115cms					
Affected Version(s): 4.2					
Unrestricted Upload of File with Dangerous Type	10-Mar-2023	7.2	A vulnerability was found in Guizhou 115cms 4.2. It has been classified as problematic. Affected is an unknown function of the file /admin/content/index. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may	N/A	A-115-115C-280323/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. VDB-222738 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1328**		
Vendor: 3DS					
Product: enovia_live_collaboration					
Affected Version(s): From (including) v6r2013xe Up to (excluding) v6r2013xe_fp.cfa.2240					
Improper Control of Generation of Code ('Code Injection')	09-Mar-2023	9.8	An XSL template vulnerability in ENOVIA Live Collaboration V6R2013xE allows Remote Code Execution. **CVE ID : CVE-2023-1287**	https://www.3ds.com/vulnerability/advisories	A-3DS-ENOV-280323/3
Improper Restriction of XML External Entity Reference	09-Mar-2023	7.5	An XML External Entity injection (XXE) vulnerability in ENOVIA Live Collaboration V6R2013xE allows an attacker to read local files on the server. **CVE ID : CVE-2023-1288**	https://www.3ds.com/vulnerability/advisories	A-3DS-ENOV-280323/4
Vendor: a2hosting					
Product: a2_optimized					
Affected Version(s): * Up to (excluding) 3.0.5					
Cross-Site Request Forgery (CSRF)	13-Mar-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in A2 Hosting A2 Optimized WP plugin <= 3.0.4 versions.	N/A	A-A2H-A2_O-280323/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23711		
Vendor: a3rev					
Product: contact_us_page_-_contact_people					
Affected Version(s): * Up to (excluding) 3.7.1					
Cross-Site Request Forgery (CSRF)	01-Mar-2023	6.5	Cross-Site Request Forgery (CSRF) vulnerability in a3rev Software Contact Us Page – Contact People plugin <= 3.7.0. **CVE ID : CVE-2023-23973**	N/A	A-A3R-CONT-280323/6
Vendor: ABB					
Product: symphony_plus_s\+_operations					
Affected Version(s): 2.1					
Improper Authentication	02-Mar-2023	8.8	Improper Authentication vulnerability in ABB Symphony Plus S+ Operations.This issue affects Symphony Plus S+ Operations: from 2.X through 2.1 SP2, 2.2, from 3.X through 3.3 SP1, 3.3 SP2. **CVE ID : CVE-2023-0228**	https://search.abb.com/library/Download.aspx?DocumentID=7PAA006722&LanguageCode=en&DocumentPartId=&Action=Launch	A-ABB-SYMP-280323/7
Affected Version(s): 2.2					
Improper Authentication	02-Mar-2023	8.8	Improper Authentication vulnerability in ABB Symphony Plus S+ Operations.This issue affects Symphony Plus S+ Operations: from 2.X through 2.1 SP2, 2.2,	https://search.abb.com/library/Download.aspx?DocumentID=7PAA006722&LanguageCode=en&DocumentPartId	A-ABB-SYMP-280323/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 3.X through 3.3 SP1, 3.3 SP2. **CVE ID : CVE-2023-0228**	=&Action=Launch	
Affected Version(s): 3.3					
Improper Authentication	02-Mar-2023	8.8	Improper Authentication vulnerability in ABB Symphony Plus S+ Operations.This issue affects Symphony Plus S+ Operations: from 2.X through 2.1 SP2, 2.2, from 3.X through 3.3 SP1, 3.3 SP2. **CVE ID : CVE-2023-0228**	https://search.abb.com/library/Download.aspx?DocumentID=7PAA006722&LanguageCode=en&DocumentPartId=&Action=Launch	A-ABB-SYMP-280323/9
Affected Version(s): From (including) 2.0 Up to (excluding) 2.1					
Improper Authentication	02-Mar-2023	8.8	Improper Authentication vulnerability in ABB Symphony Plus S+ Operations.This issue affects Symphony Plus S+ Operations: from 2.X through 2.1 SP2, 2.2, from 3.X through 3.3 SP1, 3.3 SP2. **CVE ID : CVE-2023-0228**	https://search.abb.com/library/Download.aspx?DocumentID=7PAA006722&LanguageCode=en&DocumentPartId=&Action=Launch	A-ABB-SYMP-280323/10
Affected Version(s): From (including) 3.0 Up to (excluding) 3.3					
Improper Authentication	02-Mar-2023	8.8	Improper Authentication vulnerability in ABB Symphony Plus S+ Operations.This issue affects Symphony Plus S+ Operations: from 2.X	https://search.abb.com/library/Download.aspx?DocumentID=7PAA006722&LanguageCode=en&Doc	A-ABB-SYMP-280323/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 2.1 SP2, 2.2, from 3.X through 3.3 SP1, 3.3 SP2. **CVE ID : CVE-2023-0228**	umentPartId=&Action=Launch	
Vendor: advanced_recent_posts_project					
Product: advanced_recent_posts					
Affected Version(s): * Up to (including) 0.6.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The Advanced Recent Posts WordPress plugin through 0.6.14 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0212**	N/A	A-ADV-ADVA-280323/12
Vendor: agentejo					
Product: cockpit					
Affected Version(s): * Up to (including) 2.3.9					
Use of Platform-Dependent Third Party Components	03-Mar-2023	5.5	Use of Platform-Dependent Third Party Components in GitHub repository cockpit-hq/cockpit prior to 2.4.0. **CVE ID : CVE-2023-1160**	https://huntr.dev/bounties/3ce480dc-1b1c-4230-9287-0dc3b31c2f87, https://github.com/cockpit-hq/cockpit/c	A-AGE-COCK-280323/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ommit/690016208850f2d788ebc3c67884d4c692587eb8	
Affected Version(s): * Up to (including) 2.4.0					
Unrestricted Upload of File with Dangerous Type	10-Mar-2023	8.8	Unrestricted Upload of File with Dangerous Type in GitHub repository cockpit-hq/cockpit prior to 2.4.1. **CVE ID : CVE-2023-1313**	https://hunter.dev/bounties/f73eef49-004f-4b3b-9717-90525e65ba61, https://github.com/cockpit-hq/cockpit/commit/beccca806c7071ecc732521bb5ad0bb9c64299592	A-AGE-COCK-280323/14
Vendor: agilebio					
Product: electronic_lab_notebook					
Affected Version(s): 4.234					
N/A	06-Mar-2023	8.8	AgileBio Electronic Lab Notebook v4.234 was discovered to contain a local file inclusion vulnerability. **CVE ID : CVE-2023-24217**	https://labcollector.com/labcollector-lims/add-ons/eln-electronic-lab-notebook/	A-AGI-ELEC-280323/15
Vendor: akinsoft					
Product: wolvox					
Affected Version(s): * Up to (excluding) 8.02.03					
Improper Neutralization of Special	09-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL	N/A	A-AKI-WOLV-280323/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Command ('SQL Injection') vulnerability in Akinsoft Wolvox. This issue affects Wolvox: before 8.02.03. **CVE ID : CVE-2023-1251**		
Vendor: alpatateknoloji					
Product: licensed_warehousing_automation_system					
Affected Version(s): * Up to (including) 2023.1.01					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alpata Licensed Warehousing Automation System allows Command Line Execution through SQL Injection.This issue affects Licensed Warehousing Automation System: through 2023.1.01. **CVE ID : CVE-2023-1091**	N/A	A-ALP-LICE-280323/17
Vendor: Amazon					
Product: opensearch					
Affected Version(s): * Up to (excluding) 1.3.9					
Observable Discrepancy	02-Mar-2023	5.3	OpenSearch Security is a plugin for OpenSearch that offers encryption, authentication and authorization. There	https://github.com/opensearch-project/security/security/advisories/	A-AMA-OPEN-280323/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is an observable discrepancy in the authentication response time between calls where the user provided exists and calls where it does not. This issue only affects calls using the internal basic identity provider (IdP), and not other externally configured IdPs. Patches were released in versions 1.3.9 and 2.6.0, there are no workarounds. **CVE ID : CVE-2023-25806**	GHSA-c6wg-cm5x-rqvj	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.6.0					
Observable Discrepancy	02-Mar-2023	5.3	OpenSearch Security is a plugin for OpenSearch that offers encryption, authentication and authorization. There is an observable discrepancy in the authentication response time between calls where the user provided exists and calls where it does not. This issue only affects calls using the internal basic identity provider (IdP), and not other externally configured IdPs. Patches were released in versions	https://github.com/opensearch-project/security/security/advisories/GHSA-c6wg-cm5x-rqvj	A-AMA-OPEN-280323/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.3.9 and 2.6.0, there are no workarounds. **CVE ID : CVE-2023-25806**		
Product: opensearch_security					
Affected Version(s): * Up to (excluding) 1.3.9					
Observable Discrepancy	02-Mar-2023	5.3	OpenSearch Security is a plugin for OpenSearch that offers encryption, authentication and authorization. There is an observable discrepancy in the authentication response time between calls where the user provided exists and calls where it does not. This issue only affects calls using the internal basic identity provider (IdP), and not other externally configured IdPs. Patches were released in versions 1.3.9 and 2.6.0, there are no workarounds. **CVE ID : CVE-2023-25806**	https://github.com/opensearch-project/security/security/advisories/GHSA-c6wg-cm5x-rqvj	A-AMA-OPEN-280323/20
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.6.0					
Observable Discrepancy	02-Mar-2023	5.3	OpenSearch Security is a plugin for OpenSearch that offers encryption, authentication and authorization. There is an observable discrepancy in the authentication	https://github.com/opensearch-project/security/security/advisories/GHSA-c6wg-cm5x-rqvj	A-AMA-OPEN-280323/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response time between calls where the user provided exists and calls where it does not. This issue only affects calls using the internal basic identity provider (IdP), and not other externally configured IdPs. Patches were released in versions 1.3.9 and 2.6.0, there are no workarounds. **CVE ID : CVE-2023-25806**		
Vendor: answer					
Product: answer					
Affected Version(s): * Up to (excluding) 1.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1237**	https://hunt r.dev/bounti es/cc2aa618 -05da-495d- a5cd- 51c40557d4 81, https://githu b.com/answ erdev/answ er/commit/ 0566894a2c 0e13cf07d87 7f41467e2e 21529fee8	A-ANS-ANSW-280323/22
Improper Neutralization of Input During Web Page Generation	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	https://hunt r.dev/bounti es/52f97267 -1439-4bb6- 862b- 89b8fafce50 d,	A-ANS-ANSW-280323/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-1238**	https://github.com/answerdev/answer/commit/0566894a2c0e13cf07d877f41467e2e21529fee8	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1240**	https://hunt r.dev/bounties/a24f57a4-22e3-4a17-8227-6a410a11498a, https://github.com/answerdev/answer/commit/90bfa0dcc7b49482f1d1e31aee3ab073f3c13dd9	A-ANS-ANSW-280323/24
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1241**	https://hunt r.dev/bounties/e0e9b1bb-3025-4b9f-acb4-16a5da28aa3c, https://github.com/answerdev/answer/commit/90bfa0dcc7b49482f1d1e31aee3ab073f3c13dd9	A-ANS-ANSW-280323/25
Improper Neutralization of Input During	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6.	https://github.com/answerdev/answer/commit/90bfa0dcc7b	A-ANS-ANSW-280323/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-1242**	49482f1d1e31aee3ab073f3c13dd9, https://hunter.dev/bounties/71c24c5e-ceb2-45cf-bda7-fa195d37e289	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1244**	https://github.com/answerdev/answer/commit/9870ed87fb24ed468aaf1e169c2d028e0f375106, https://hunter.dev/bounties/bcab9555-8a35-42b2-a7de-0a79fd710b52	A-ANS-ANSW-280323/27
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1245**	https://hunter.dev/bounties/f8011bb3-8212-4937-aa58-79f4b73be004, https://github.com/answerdev/answer/commit/71a4cdac811129759691 29d308899edd155c0e80	A-ANS-ANSW-280323/28
Improper Neutralization of	07-Mar-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository	https://github.com/answerdev/answ	A-ANS-ANSW-280323/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1239**	er/commit/9870ed87fb24ed468aaf1e169c2d028e0f375106, https://hunter.dev/bounties/3a22c609-d2d8-4613-815d-58f5990b8bd8	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository answerdev/answer prior to 1.0.6. **CVE ID : CVE-2023-1243**	https://github.com/answerdev/answer/commit/9870ed87fb24ed468aaf1e169c2d028e0f375106, https://hunter.dev/bounties/1d62d35a-b096-4b76-a021-347c3f1c570c	A-ANS-ANSW-280323/30
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (excluding) 2.5.2					
Generation of Error Message Containing Sensitive Information	15-Mar-2023	5.3	Generation of Error Message Containing Sensitive Information vulnerability in Apache Software Foundation Apache Airflow.This issue affects Apache Airflow: before 2.5.2. **CVE ID : CVE-2023-25695**	https://github.com/apache/airflow/pull/29501, https://lists.apache.org/thread/z8w6ckzs61ql365tv4d19k82o67r15p2	A-APA-AIRF-280323/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dubbo					
Affected Version(s): From (including) 2.7.0 Up to (including) 2.7.21					
Deserialization of Untrusted Data	08-Mar-2023	9.8	A deserialization vulnerability existed when dubbo generic invoke, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.21 and prior versions; Apache Dubbo 3.0.x version 3.0.13 and prior versions; Apache Dubbo 3.1.x version 3.1.5 and prior versions. **CVE ID : CVE-2023-23638**	https://lists.apache.org/thread/8h6zscfzj482z512d2v5ft63hdhzm0cb	A-APA-DUBB-280323/32
Affected Version(s): From (including) 3.0.0 Up to (including) 3.0.13					
Deserialization of Untrusted Data	08-Mar-2023	9.8	A deserialization vulnerability existed when dubbo generic invoke, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.21 and prior versions; Apache Dubbo 3.0.x version 3.0.13 and prior versions; Apache Dubbo 3.1.x version 3.1.5 and prior versions. **CVE ID : CVE-2023-23638**	https://lists.apache.org/thread/8h6zscfzj482z512d2v5ft63hdhzm0cb	A-APA-DUBB-280323/33
Affected Version(s): From (including) 3.1.0 Up to (including) 3.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	08-Mar-2023	9.8	A deserialization vulnerability existed when dubbo generic invoke, which could lead to malicious code execution. This issue affects Apache Dubbo 2.7.x version 2.7.21 and prior versions; Apache Dubbo 3.0.x version 3.0.13 and prior versions; Apache Dubbo 3.1.x version 3.1.5 and prior versions. **CVE ID : CVE-2023-23638**	https://lists.apache.org/thread/8h6zscfzj482z512d2v5ft63hdhzm0cb	A-APA-DUBB-280323/34
Product: http_server					
Affected Version(s): From (including) 2.4.0 Up to (including) 2.4.55					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	07-Mar-2023	9.8	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable	https://httpd.apache.org/security/vulnerabilities_24.html	A-APA-HTTP-280323/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server. **CVE ID : CVE-2023-25690**		
Affected Version(s): From (including) 2.4.30 Up to (including) 2.4.55					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	07-Mar-2023	7.5	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the	https://httpd.apache.org/security/vulnerabilities_24.html	A-APA-HTTP-280323/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response forwarded to the client. **CVE ID : CVE-2023-27522**		
Product: log4j					
Affected Version(s): From (including) 1.0.4 Up to (excluding) 2.0					
Deserialization of Untrusted Data	10-Mar-2023	7.5	** UNSUPPORTED WHEN ASSIGNED ** When using the Chainsaw or SocketAppender components with Log4j 1.x on JRE less than 1.7, an attacker that manages to cause a logging entry involving a specially-crafted (ie, deeply nested) hashmap or hashtable (depending on which logging component is in use) to be processed could exhaust the available memory in the virtual machine and achieve Denial of Service when the object is deserialized. This issue affects Apache Log4j before 2. Affected users are recommended to update to Log4j 2.x. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	N/A	A-APA-LOG4-280323/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26464		
Vendor: ARM					
Product: aarch64cryptolib					
Affected Version(s): * Up to (excluding) 2023-02-20					
Improper Initialization	15-Mar-2023	3.7	The armv8_dec_aes_gcm_full() API of Arm AArch64cryptolib before 86065c6 fails to the verify the authentication tag of AES-GCM protected data, leading to a man-in-the-middle attack. This occurs because of an improperly initialized variable. **CVE ID : CVE-2023-26084**	https://github.com/ARM-software/AArch64cryptolib/security/advisories/GHSA-47c6-7x5x-r74g	A-ARM-AARC-280323/38
Vendor: art_gallery_management_system_project					
Product: art_gallery_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Mar-2023	9.8	Art Gallery Management System v1.0 was discovered to contain a SQL injection vulnerability via the viewid parameter on the enquiry page. **CVE ID : CVE-2023-24726**	https://github.com/rahulpatwari/CVE/blob/main/CVE-2023-24726/CVE-2023-24726.txt	A-ART-ART_-280323/39
Vendor: Arubanetworks					
Product: sd-wan					
Affected Version(s): From (including) 8.7.0.0-2.3.0.0 Up to (including) 8.7.0.0-2.3.0.8					
Improper Neutralizat	01-Mar-2023	9.8	There are multiple command injection	https://www.arubanetw	A-ARU-SD-W-280323/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22747**	orks.com/assets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22748**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22749**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/42
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22750**		
Out-of-bounds Write	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22751**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/44
Buffer Copy without Checking Size of Input ('Classic	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22752**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22753**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/46
Buffer Copy without Checking	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying	https://www.arubanetworks.com/assets/alert/A	A-ARU-SD-W-280323/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22754**	RUBA-PSA-2023-002.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22755**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22756**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/49
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22757**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22758**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/51
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22759**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22760**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/53
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22761**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/55
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/57
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/58
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/60
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/61
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	A-ARU-SD-W-280323/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/63
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22772**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/65
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/66
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	A vulnerability exists which allows an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22775		
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	An authenticated information disclosure vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22777**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/68
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/69
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	4.8	A vulnerability in the ArubaOS web management interface could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-22778**		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	A-ARU-SD-W-280323/71
Vendor: asosegitim					
Product: bookcites					
Affected Version(s): * Up to (excluding) 23.01.05					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ASOS Information Technologies Book Cites allows Cross-Site Scripting (XSS).This issue	N/A	A-ASO-BOOK-280323/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Book Cites: before 23.01.05. **CVE ID : CVE-2023-0578**		
Product: sobiad					
Affected Version(s): * Up to (excluding) 23.02.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ASOS Information Technologies SOBIAD allows Cross-Site Scripting (XSS).This issue affects SOBIAD: before 23.02.01. **CVE ID : CVE-2023-0577**	N/A	A-ASO-SOBI-280323/73
Vendor: autoaffiliatelinks					
Product: auto_affiliate_links					
Affected Version(s): * Up to (excluding) 6.3.0.3					
Cross-Site Request Forgery (CSRF)	13-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Lucian Apostol Auto Affiliate Links plugin <= 6.3.0.2 versions. **CVE ID : CVE-2023-25973**	N/A	A-AUT-AUTO-280323/74
Vendor: avantfax					
Product: avantfax					
Affected Version(s): 3.3.7					
Unrestricted Upload of File with	10-Mar-2023	8.8	A File Upload vulnerability exists in AvantFAX 3.3.7.	http://avantfax.com	A-AVA-AVAN-280323/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			An authenticated user can bypass PHP file type validation in FileUpload.php by uploading a specially crafted PHP file. **CVE ID : CVE-2023-23328**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	A Stored Cross-Site Scripting (XSS) vulnerability exists in AvantFAX 3.3.7. An authenticated low privilege user can inject arbitrary Javascript into their e-mail address which is executed when an administrator logs into AvantFAX to view the admin dashboard. This may result in stealing an administrator's session cookie and hijacking their session. **CVE ID : CVE-2023-23326**	http://avantfax.com	A-AVA-AVAN-280323/76
Exposure of Sensitive Information to an Unauthorized Actor	10-Mar-2023	4.9	An Information Disclosure vulnerability exists in AvantFAX 3.3.7. Backups of the AvantFAX sent/received faxes, and database backups are stored using the current date as the filename and hosted on the	N/A	A-AVA-AVAN-280323/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web server without access controls. **CVE ID : CVE-2023-23327**		
Vendor: best_pos_management_system_project					
Product: best_pos_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /kruxton/receipt.php. **CVE ID : CVE-2023-27202**	N/A	A-BES-BEST-280323/78
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /billing/home.php. **CVE ID : CVE-2023-27203**	N/A	A-BES-BEST-280323/79
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /kruxton/manage_user.php. **CVE ID : CVE-2023-27204**	N/A	A-BES-BEST-280323/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Best POS Management System 1.0 was discovered to contain a SQL injection vulnerability via the month parameter at /kruxton/sales_report.php. **CVE ID : CVE-2023-27205**	N/A	A-BES-BEST-280323/81
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in /kruxton/navbar.php of Best POS Management System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the page parameter. **CVE ID : CVE-2023-27206**	N/A	A-BES-BEST-280323/82
Vendor: bitwarden					
Product: bitwarden					
Affected Version(s): * Up to (including) 2023.2.1					
N/A	09-Mar-2023	7.5	** DISPUTED ** Bitwarden through 2023.2.1 offers password auto-fill when the second-level domain matches, e.g., a password stored for an example.com hosting provider when customer-website.example.com is visited. NOTE: the vendor's position is that "Auto-fill on	N/A	A-BIT-BITW-280323/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page load" is not enabled by default. **CVE ID : CVE-2023-27974**		
Vendor: Blogengine					
Product: blogengine.net					
Affected Version(s): 3.3.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	A stored Cross-site Scripting (XSS) vulnerability in BlogEngine.NET 3.3.8.0, allows injection of arbitrary JavaScript in the security context of a blog visitor through an upload of a specially crafted file. **CVE ID : CVE-2023-22856**	N/A	A-BLO-BLOG-280323/84
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	A stored Cross-site Scripting (XSS) vulnerability in BlogEngine.NET 3.3.8.0, allows injection of arbitrary JavaScript in the security context of a blog visitor through an injection of a malicious payload into a blog post. **CVE ID : CVE-2023-22857**	N/A	A-BLO-BLOG-280323/85
N/A	06-Mar-2023	5.3	An Improper Access Control vulnerability in BlogEngine.NET 3.3.8.0, allows unauthenticated visitors to access the	N/A	A-BLO-BLOG-280323/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files of unpublished blogs. **CVE ID : CVE-2023-22858**		
Vendor: bp_monitoring_management_system_project					
Product: bp_monitoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	9.8	BP Monitoring Management System v1.0 was discovered to contain a SQL injection vulnerability via the emailid parameter in the login page. **CVE ID : CVE-2023-27074**	N/A	A-BP_-BP_M-280323/87
Vendor: btcpayserver					
Product: btcpayserver					
Affected Version(s): * Up to (excluding) 1.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	5.4	Command Injection in GitHub repository btcpayserver/btcpayserver prior to 1.8.3. **CVE ID : CVE-2023-1270**	https://github.com/btcpayserver/btcpayserver/commit/7b5ce8f70c060b01990d3f7109e97e0144d878a4, https://huntr.dev/bounties/ad1f917f-2b25-40ef-9215-c805354c683b	A-BTC-BTCP-280323/88
Product: btcpay_server					
Affected Version(s): * Up to (excluding) 1.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Equivalent Special Elements	02-Mar-2023	5.4	Improper Neutralization of Equivalent Special Elements in GitHub repository btcpayserver/btcpayserver prior to 1.8.0. **CVE ID : CVE-2023-1149**	https://github.com/btcpayserver/btcpayserver/commit/ddb125f45892b4dafdbd5c072af1ce623758bb92, https://hunt r.dev/bounties/2e734209-d7b0-4f57-a8be-c65c82208f2f	A-BTC-BTCP-280323/89
Vendor: builder					
Product: qwik					
Affected Version(s): * Up to (excluding) 0.21.0					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	9.8	Code Injection in GitHub repository builderio/qwik prior to 0.21.0. **CVE ID : CVE-2023-1283**	https://hunt r.dev/bounties/63f1ff91-48f3-4886-a179-103f1ddd8ff8, https://github.com/builderio/qwik/commit/4d9ba6e098ae6e537aa55abb6b8369bb670ffe66	A-BUI-QWIK-280323/90
Vendor: bumsys_project					
Product: bumsys					
Affected Version(s): * Up to (excluding) 2.0.2					
Improper Neutralization of Special	13-Mar-2023	6.5	SQL Injection in GitHub repository unilogies/bumsys prior to v2.0.2.	https://hunt r.dev/bounties/1b1dbc5a-df16-421f-	A-BUM-BUMS-280323/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			**CVE ID : CVE-2023-1361**	9a0d-de83e43146c4, https://github.com/unilogies/bumsys/commit/6a328eb5bf9dbb44329a3df82e95683b77c4730d	
Improper Restriction of Rendered UI Layers or Frames	13-Mar-2023	6.1	Improper Restriction of Rendered UI Layers or Frames in GitHub repository unilogies/bumsys prior to v2.0.2. **CVE ID : CVE-2023-1362**	https://github.com/unilogies/bumsys/commit/8c5b27d54707f9805b27ef26ad741f2801e30e1f, https://hunt r.dev/bounties/e5959166-c8ef-4ada-9bb1-0ff5a9693bac	A-BUM-BUMS-280323/92
Vendor: bytecodealliance					
Product: cranelift-codegen					
Affected Version(s): 0.92.0					
Out-of-bounds Read	08-Mar-2023	9.9	wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/commit/63fb30e4b44154	A-BYT-CRAN-280323/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7ffffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are	55d47b3da5a19d79c12f4f2d1f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst`		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example. **CVE ID : CVE-2023-26489**		
Off-by-one Error	08-Mar-2023	4.3	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select` instruction which will produce the wrong results when	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA	A-BYT-CRAN-280323/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as AArch64 and s390x are not affected. **CVE ID : CVE-2023-27477**	-xm67-587q-r2vw	
Affected Version(s): 0.93.0					
Out-of-bounds Read	08-Mar-2023	9.9	wasmtime is a fast and secure runtime for WebAssembly. In affected versions	https://groups.google.com/a/bytecodealliance.or	A-BYT-CRAN-280323/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7ffffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder,	g/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/commit/63fb30e4b4415455d47b3da5a19d79c12f4f2d1f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example. **CVE ID : CVE-2023-26489**		
Off-by-one Error	08-Mar-2023	4.3	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code	https://groups.google.com/a/bytecodealliance.or	A-BYT-CRAN-280323/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select` instruction which will produce the wrong results when the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as	g/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-xm67-587q-r2vw	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AArch64 and s390x are not affected. **CVE ID : CVE-2023-27477**		
Affected Version(s): From (including) 0.84.0 Up to (excluding) 0.91.1					
Out-of-bounds Read	08-Mar-2023	9.9	wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7ffffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/commit/63fb30e4b4415455d47b3da5a19d79c12f4f2d1f	A-BYT-CRAN-280323/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cranelift's AArch64 backend, for example. **CVE ID : CVE-2023-26489**		
Off-by-one Error	08-Mar-2023	4.3	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select` instruction which will produce the wrong results when the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-xm67-587q-r2vw	A-BYT-CRAN-280323/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as AArch64 and s390x are not affected. **CVE ID : CVE-2023-27477**		
Product: wasmtime					
Affected Version(s): 5.0.0					
Out-of-bounds Read	08-Mar-2023	9.9	wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however,	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/commit/63fb30e4b4415455d47b3da5a19d79c12f4f2d1f	A-BYT-WASM-280323/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addresses up to `0xffffffff * 8 + 0x7fffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example. **CVE ID : CVE-2023-26489**		
Off-by-one Error	08-Mar-2023	4.3	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select` instruction which will produce the wrong results when the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-xm67-587q-r2vw	A-BYT-WASM-280323/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as AArch64 and s390x are not affected. **CVE ID : CVE-2023-27477**		
Affected Version(s): 6.0.0					
Out-of-bounds Read	08-Mar-2023	9.9	wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/commit/63fb30e4b4415455d47b3da5a19d79c12f4f2d1f	A-BYT-WASM-280323/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7fffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value. Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memory_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example. **CVE ID : CVE-2023-26489**		
Off-by-one Error	08-Mar-2023	4.3	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select` instruction which will produce the wrong results when the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/wasmtime/security/advisories/GHSA-xm67-587q-r2vw	A-BYT-WASM-280323/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as AArch64 and s390x are not affected. **CVE ID : CVE-2023-27477**		
Affected Version(s): From (including) 0.37.0 Up to (excluding) 4.0.1					
Out-of-bounds Read	08-Mar-2023	9.9	wasmtime is a fast and secure runtime for WebAssembly. In affected versions wasmtime's code generator, Cranelift, has a bug on x86_64 targets where address-mode computation	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/	A-BYT-WASM-280323/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mistakenly would calculate a 35-bit effective address instead of WebAssembly's defined 33-bit effective address. This bug means that, with default codegen settings, a wasm-controlled load/store operation could read/write addresses up to 35 bits away from the base of linear memory. Due to this bug, however, addresses up to `0xffffffff * 8 + 0x7fffffc = 36507222004 = ~34G` bytes away from the base of linear memory are possible from guest code. This means that the virtual memory 6G away from the base of linear memory up to ~34G away can be read/written by a malicious module. A guest module can, without the knowledge of the embedder, read/write memory in this region. The memory may belong to other WebAssembly instances when using	wasmtime/commit/63fb30e4b4415455d47b3da5a19d79c12f4f2d1f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the pooling allocator, for example. Affected embedders are recommended to analyze preexisting wasm modules to see if they're affected by the incorrect codegen rules and possibly correlate that with an anomalous number of traps during historical execution to locate possibly suspicious modules. The specific bug in Cranelift's x86_64 backend is that a WebAssembly address which is left-shifted by a constant amount from 1 to 3 will get folded into x86_64's addressing modes which perform shifts. For example `(i32.load (i32.shl (local.get 0) (i32.const 3)))` loads from the WebAssembly address `$local0 << 3`. When translated to Cranelift the `$local0 << 3` computation, a 32-bit value, is zero-extended to a 64-bit value and then added to the base address of linear memory. Cranelift would generate an		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instruction of the form `movl (%base, %local0, 8), %dst` which calculates `%base + %local0 << 3`. The bug here, however, is that the address computation happens with 64-bit values, where the `$local0 << 3` computation was supposed to be truncated to a a 32-bit value. This means that `%local0`, which can use up to 32-bits for an address, gets 3 extra bits of address space to be accessible via this `movl` instruction. The fix in Cranelift is to remove the erroneous lowering rules in the backend which handle these zero-extended expression. The above example is then translated to `movl %local0, %temp; shl $3, %temp; movl (%base, %temp), %dst` which correctly truncates the intermediate computation of `%local0 << 3` to 32-bits inside the `%temp` register which is then added to the `%base` value.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Wasmtime version 4.0.1, 5.0.1, and 6.0.1 have been released and have all been patched to no longer contain the erroneous lowering rules. While updating Wasmtime is recommended, there are a number of possible workarounds that embedders can employ to mitigate this issue if updating is not possible. Note that none of these workarounds are on-by-default and require explicit configuration: 1. The `Config::static_memory_maximum_size(0)` option can be used to force all accesses to linear memory to be explicitly bounds-checked. This will perform a bounds check separately from the address-mode computation which correctly calculates the effective address of a load/store. Note that this can have a large impact on the execution performance of WebAssembly modules. 2. The `Config::static_memo		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ry_guard_size(1 << 36)` option can be used to greatly increase the guard pages placed after linear memory. This will guarantee that memory accesses up-to-34G away are guaranteed to be semantically correct by reserving unmapped memory for the instance. Note that this reserves a very large amount of virtual memory per-instances and can greatly reduce the maximum number of concurrent instances being run. 3. If using a non-x86_64 host is possible, then that will also work around this bug. This bug does not affect Wasmtime's or Cranelift's AArch64 backend, for example. **CVE ID : CVE-2023-26489**		
Off-by-one Error	08-Mar-2023	4.3	wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's code generation backend, Cranelift, has a bug on x86_64 platforms for the WebAssembly `i8x16.select`	https://groups.google.com/a/bytecodealliance.org/g/sec-announce/c/Mov-ItrNJsQ, https://github.com/bytecodealliance/	A-BYT-WASM-280323/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			instruction which will produce the wrong results when the same operand is provided to the instruction and some of the selected indices are greater than 16. There is an off-by-one error in the calculation of the mask to the `pshufb` instruction which causes incorrect results to be returned if lanes are selected from the second vector. This codegen bug has been fixed in Wasmtiem 6.0.1, 5.0.1, and 4.0.1. Users are recommended to upgrade to these updated versions. If upgrading is not an option for you at this time, you can avoid this miscompilation by disabling the Wasm simd proposal. Additionally the bug is only present on x86_64 hosts. Other platforms such as AArch64 and s390x are not affected. **CVE ID : CVE-2023-27477**	wasmtime/security/advisories/GHSA-xm67-587q-r2vw	
Vendor: campaign_url_builder_project					
Product: campaign_url_builder					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Mar-2023	5.4	The Campaign URL Builder WordPress plugin before 1.8.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0538**	N/A	A-CAM-CAMP-280323/105
Vendor: Cisco					
Product: email_security_appliance					
Affected Version(s): * Up to (excluding) 12.5.3-041					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Affected Version(s): From (including) 12.5.0 Up to (excluding) 12.5.3-041					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-2023	6.7	Vulnerability in the CLI of Cisco Secure Email Gateway could allow an authenticated, remote attacker to execute arbitrary commands. These vulnerability is due to improper input validation in the CLI. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials. **CVE ID : CVE-2023-20075**		
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.0.5-007					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-2023	6.7	Vulnerability in the CLI of Cisco Secure Email Gateway could allow an authenticated, remote attacker to execute arbitrary commands. These vulnerability is due to improper input validation in the CLI. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials. **CVE ID : CVE-2023-20075**		
Affected Version(s): From (including) 13.5.0 Up to (excluding) 13.5.4-038					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-2023	6.7	Vulnerability in the CLI of Cisco Secure Email Gateway could allow an authenticated, remote attacker to execute arbitrary commands. These vulnerability is due to improper input validation in the CLI. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20075		
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.2.1-020					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain root access on the device. **CVE ID : CVE-2023-20009**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Mar-2023	6.7	Vulnerability in the CLI of Cisco Secure Email Gateway could allow an authenticated, remote attacker to execute arbitrary commands. These vulnerability is due to improper input validation in the CLI. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials. **CVE ID : CVE-2023-20075**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-EMAI-280323/113
Affected Version(s): From (including) 14.3.0 Up to (excluding) 14.3.0-032					
Unrestricted Upload of File with	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of	https://sec.cloudapps.cisco.com/secu	A-CIS-EMAI-280323/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**	rity/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	
Improper Neutralizat	01-Mar-2023	6.7	Vulnerability in the CLI of Cisco Secure	https://sec.cloudapps.cis	A-CIS-EMAI-280323/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			Email Gateway could allow an authenticated, remote attacker to execute arbitrary commands. These vulnerability is due to improper input validation in the CLI. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials. **CVE ID : CVE-2023-20075**	co.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	
Product: evolved_programmable_network_manager					
Affected Version(s): * Up to (excluding) 7.0					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	5.4	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-	A-CIS-EVOL-280323/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need to have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20069**	epnm-xss-mZShH2J	
Product: finesse					
Affected Version(s): * Up to (excluding) 12.6\\(1\\)					
N/A	03-Mar-2023	7.5	A vulnerability in the nginx configurations that are provided as	https://sec.cloudapps.cisco.com/secu	A-CIS-FINE-280323/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			part of the VPN-less reverse proxy for Cisco Finesse could allow an unauthenticated, remote attacker to create a denial of service (DoS) condition for new and existing users who are connected through a load balancer. This vulnerability is due to improper IP address filtering by the reverse proxy. An attacker could exploit this vulnerability by sending a series of unauthenticated requests to the reverse proxy. A successful exploit could allow the attacker to cause all current traffic and subsequent requests to the reverse proxy through a load balancer to be dropped, resulting in a DoS condition. **CVE ID : CVE-2023-20088**	rity/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-proxy-dos-vY5dQhrV	
Affected Version(s): 12.6\\(1\\)					
N/A	03-Mar-2023	7.5	A vulnerability in the nginx configurations that are provided as part of the VPN-less reverse proxy for Cisco Finesse could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-FINE-280323/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, remote attacker to create a denial of service (DoS) condition for new and existing users who are connected through a load balancer. This vulnerability is due to improper IP address filtering by the reverse proxy. An attacker could exploit this vulnerability by sending a series of unauthenticated requests to the reverse proxy. A successful exploit could allow the attacker to cause all current traffic and subsequent requests to the reverse proxy through a load balancer to be dropped, resulting in a DoS condition. **CVE ID : CVE-2023-20088**	visory/cisco-sa-finesse-proxy-dos-vY5dQhrV	
Product: identity_services_engine					
Affected Version(s): 3.2					
Improper Neutralization of Input During Web Page Generation	01-Mar-2023	6.1	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-IDEN-280323/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20085**	sa-ise-xss-ubfHG75C	
Product: nexus_dashboard					
Affected Version(s): * Up to (excluding) 2.3\\(1c\\)					
Uncontrolled Resource Consumption	01-Mar-2023	7.5	A vulnerability in the DNS functionality of Cisco Nexus Dashboard Software could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-NEXU-280323/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition. This vulnerability is due to the improper processing of DNS requests. An attacker could exploit this vulnerability by sending a continuous stream of DNS requests to an affected device. A successful exploit could allow the attacker to cause the coredns service to stop working or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2023-20014**	sa-ndb-dnsdos-bYscZOsu	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	6.1	A vulnerability in the web-based management interface of Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability is due to insufficient user input validation. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nexus-dashboard-xss-xc5BcgsQ	A-CIS-NEXU-280323/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20053**		
Product: packaged_contact_center_enterprise					
Affected Version(s): -					
Exposure of Resource to Wrong Sphere	03-Mar-2023	6.5	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20061**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	A-CIS-PACK-280323/122
Server-Side Request Forgery (SSRF)	03-Mar-2023	4.3	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-PACK-280323/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20062**	visory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	
Product: prime_infrastructure					
Affected Version(s): * Up to (excluding) 3.10.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	5.4	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-epnm-xss-mZShH2J	A-CIS-PRIM-280323/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need to have valid credentials to access the web-based management interface of the affected device. **CVE ID : CVE-2023-20069**		
Product: secure_email_and_web_manager					
Affected Version(s): * Up to (excluding) 12.8.1-021					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-SECU-280323/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Affected Version(s): From (including) 13.8.0 Up to (excluding) 13.8.1-108					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user credential with at least a [[privilege of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-SECU-280323/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.2.0-224					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The attacker has to have a valid user	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-SECU-280323/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Affected Version(s): From (including) 14.3.0 Up to (excluding) 14.3.0-120					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	7.2	A vulnerability in the Web UI and administrative CLI of the Cisco Secure Email Gateway (ESA) and Cisco Secure Email and Web Manager (SMA) could allow an authenticated remote attacker and or authenticated local attacker to escalate their privilege level and gain root access. The	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8	A-CIS-SECU-280323/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker has to have a valid user credential with at least a [[privilege of operator - validate actual name]]. The vulnerability is due to the processing of a specially crafted SNMP configuration file. An attacker could exploit this vulnerability by authenticating to the targeted device and uploading a specially crafted SNMP configuration file that when uploaded could allow for the execution of commands as root. An exploit could allow the attacker to gain root access on the device. **CVE ID : CVE-2023-20009**		
Product: secure_endpoint					
Affected Version(s): * Up to (excluding) 1.20.2					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CIS-SECU-280323/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Improper Restriction of Recursive Entity References in DTDs ('XML	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-	A-CIS-SECU-280323/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Expansion')			ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**	xxe-TcSZduhN	
Affected Version(s): * Up to (excluding) 1.21.1					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CIS-SECU-280323/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Improper Restriction of Recursive Entity References	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-SECU-280323/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in DTDs ('XML Entity Expansion')			vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**	visory/cisco-sa-clamav-xxe-TcSZduhN	
Affected Version(s): * Up to (excluding) 7.5.9					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CIS-SECU-280323/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Improper Restriction of Recursive	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning	https://sec.cloudapps.cisco.com/security/center/	A-CIS-SECU-280323/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity References in DTDs ('XML Entity Expansion')			library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**	content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN	
Affected Version(s): From (including) 8.0.1.21160 Up to (excluding) 8.1.5					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-SECU-280323/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**	sa-clamav-q8DThCy	
Improper Restriction	01-Mar-2023	5.3	On Feb 15, 2023, the following	https://sec.cloudapps.cis	A-CIS-SECU-280323/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Recursive Entity References in DTDs ('XML Entity Expansion')			vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**	co.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN	
Product: secure_endpoint_private_cloud					
Affected Version(s): * Up to (excluding) 3.6.0					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning	https://sec.cloudapps.cisco.com/security/center/	A-CIS-SECU-280323/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"].	content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20032		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN	A-CIS-SECU-280323/138
Product: unified_contact_center_enterprise					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Exposure of Resource to Wrong Sphere	03-Mar-2023	6.5	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20061**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	A-CIS-UNIF-280323/139
Server-Side Request Forgery (SSRF)	03-Mar-2023	4.3	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20062**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	A-CIS-UNIF-280323/140
Product: unified_contact_center_express					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	03-Mar-2023	6.5	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20061**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	A-CIS-UNIF-280323/141
Server-Side Request Forgery (SSRF)	03-Mar-2023	4.3	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20062**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	A-CIS-UNIF-280323/142
Product: unified_intelligence_center					
Affected Version(s): * Up to (excluding) 12.6\\(2\\)					
Exposure of	03-Mar-2023	6.5	Multiple vulnerabilities in	https://sec.cloudapps.cis	A-CIS-UNIF-280323/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20061**	co.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	
Server-Side Request Forgery (SSRF)	03-Mar-2023	4.3	Multiple vulnerabilities in Cisco Unified Intelligence Center could allow an authenticated, remote attacker to collect sensitive information or perform a server-side request forgery (SSRF) attack on an affected system. Cisco plans to release software updates that address these vulnerabilities. **CVE ID : CVE-2023-20062**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-infodisc-ssrf-84ZBmwVk	A-CIS-UNIF-280323/144
Product: webex_teams					
Affected Version(s): -					
Improper Neutralization of Input	03-Mar-2023	6.1	A vulnerability in the file upload functionality of Cisco Webex App for Web	https://sec.cloudapps.cisco.com/security/center/	A-CIS-WEBE-280323/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending an arbitrary file to a user and persuading that user to browse to a specific URL. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2023-20104**	content/CiscoSecurityAdvisory/cisco-sa-webex-xss-Yn8HHsMJ	
Product: web_security_appliance					
Affected Version(s): * Up to (excluding) 12.5.6					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CIS-WEB_-280323/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.0.4-005					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was	https://sec.cloudapps.cisco.com/security/center/content/Cisc	A-CIS-WEB_-280323/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**	oSecurityAdvisory/cisco-sa-clamav-q8DThCy	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 14.5.0 Up to (excluding) 14.5.1-013					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CIS-WEB_-280323/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.0-254					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CIS-WEB_-280323/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Vendor: Clamav					
Product: clamav					
Affected Version(s): * Up to (including) 0.103.7					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by submitting a crafted HFS+ partition file to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CLA-CLAM-280323/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution that may result in XML external entity	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN	A-CLA-CLAM-280323/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**		
Affected Version(s): 1.0.0					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CLA-CLAM-280323/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to enabling XML entity substitution	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN	A-CLA-CLAM-280323/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**		
Affected Version(s): From (including) 0.104.0 Up to (including) 0.105.1					
Out-of-bounds Write	01-Mar-2023	9.8	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partition file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to execute arbitrary code. This vulnerability is due to a missing buffer size check that may result in a heap buffer overflow write. An attacker	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy	A-CLA-CLAM-280323/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by submitting a crafted HFS+ partition file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the ClamAV scanning process, or else crash the process, resulting in a denial of service (DoS) condition. For a description of this vulnerability, see the ClamAV blog ["https://blog.clamav.net/"]. **CVE ID : CVE-2023-20032**		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	01-Mar-2023	5.3	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the DMG file parser of ClamAV versions 1.0.0 and earlier, 0.105.1 and earlier, and 0.103.7 and earlier could allow an unauthenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN	A-CLA-CLAM-280323/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to enabling XML entity substitution that may result in XML external entity injection. An attacker could exploit this vulnerability by submitting a crafted DMG file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to leak bytes from any file that may be read by the ClamAV scanning process. **CVE ID : CVE-2023-20052**		
Vendor: client_logo_carousel_project					
Product: client_logo_carousel					
Affected Version(s): * Up to (including) 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Mar-2023	5.4	The Client Logo Carousel WordPress plugin through 3.0.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0073**	N/A	A-CLI-CLIE-280323/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: cm-wp					
Product: auto_featured_image					
Affected Version(s): * Up to (excluding) 3.9.16					
Unrestricted Upload of File with Dangerous Type	13-Mar-2023	8.8	The Auto Featured Image (Auto Post Thumbnail) WordPress plugin before 3.9.16 includes an AJAX endpoint that allows any user with at least Author privileges to upload arbitrary files, such as PHP files. This is caused by incorrect file extension validation. **CVE ID : CVE-2023-0477**	N/A	A-CM--AUTO-280323/157
Vendor: codeermeneer					
Product: companion_sitemap_generator					
Affected Version(s): * Up to (including) 4.5.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Mar-2023	5.4	The Companion Sitemap Generator WordPress plugin through 4.5.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0066**	N/A	A-COD-COMP-280323/158

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: coderex					
Product: wp_vr					
Affected Version(s): * Up to (excluding) 8.2.8					
Cross-Site Request Forgery (CSRF)	15-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Rextheme WP VR – 360 Panorama and Virtual Tour Builder For WordPress plugin <= 8.2.7 versions. **CVE ID : CVE-2023-25708**	N/A	A-COD-WP_V-280323/159
Vendor: computer_parts_sales_and_inventory_system_project					
Product: computer_parts_sales_and_inventory_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Computer Parts Sales and Inventory System 1.0. This affects an unknown part of the file processlogin. The manipulation of the argument user 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 identifier VDB-222105 was assigned to this vulnerability. **CVE ID : CVE-2023-1130**	N/A	A-COM-COMP-280323/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Computer Parts Sales and Inventory System 1.0. This affects an unknown part of the file cust_transac.php. The manipulation of the argument phonenumber 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 identifier VDB-222849 was assigned to this vulnerability. **CVE ID : CVE-2023-1351**	N/A	A-COM-COMP-280323/161
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	6.1	A vulnerability has been found in SourceCodester Computer Parts Sales and Inventory System 1.0 and classified as problematic. This vulnerability affects unknown code of the file customer.php. The manipulation of the argument FIRST_NAME/LAST_NAME/PHONE_NUMBER leads to cross site scripting. The attack can be	N/A	A-COM-COMP-280323/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222106 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1131**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-2023	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Computer Parts Sales and Inventory System 1.0. Affected is an unknown function of the component Add Supplier Handler. The manipulation of the argument company_name/province/city/phone_number leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222330 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1179**	N/A	A-COM-COMP-280323/163
Improper Neutralization of Input	13-Mar-2023	5.4	A vulnerability, which was classified as problematic, was found in	N/A	A-COM-COMP-280323/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			SourceCodester Computer Parts Sales and Inventory System 1.0. Affected is an unknown function of the component Add User Account. The manipulation of the argument username leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222870 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1363**		
Vendor: covid_19_testing_management_system_project					
Product: covid_19_testing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file patient-report.php of the component POST Parameter Handler. The manipulation of the argument	N/A	A-COV-COVI-280323/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			searchdata leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222661 was assigned to this vulnerability. **CVE ID : CVE-2023-1300**		
Vendor: cozmoslabs					
Product: client_portal					
Affected Version(s): * Up to (excluding) 1.1.9					
Cross-Site Request Forgery (CSRF)	15-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs, Madalin Ungureanu, Antohe Cristian Client Portal – Private user pages and login plugin <= 1.1.8 versions. **CVE ID : CVE-2023-25968**	N/A	A-COZ-CLIE-280323/166
Vendor: Craftcms					
Product: craft_cms					
Affected Version(s): * Up to (excluding) 4.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	5.4	Craft is a platform for creating digital experiences. When you insert a payload inside a label name or instruction of an entry type, an cross-site scripting (XSS) happens in the quick post widget on the admin dashboard.	https://github.com/craftcms/cms/security/advisories/GHSA-qcrj-6ffc-v7hq	A-CRA-CRAF-280323/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue has been fixed in version 4.3.7. **CVE ID : CVE-2023-23927**		
Vendor: crmeb					
Product: crmeb					
Affected Version(s): * Up to (including) 1.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Mar-2023	7.2	CRMEB <=1.3.4 is vulnerable to SQL Injection via /api/admin/user/list. **CVE ID : CVE-2023-25223**	https://github.com/crmeb/crmeb_java/issues/9	A-CRM-CRME-280323/168
Affected Version(s): 1.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2023	7.2	A vulnerability was found in Zhong Bang CRMEB Java 1.3.4. It has been classified as critical. This affects an unknown part of the file /api/admin/system/store/order/list. The manipulation of the argument keywords leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-222261 was assigned to this vulnerability. **CVE ID : CVE-2023-1165**	N/A	A-CRM-CRME-280323/169
Vendor: crossplane					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: crossplane					
Affected Version(s): From (including) 1.10.0 Up to (excluding) 1.10.3					
Uncontrolled Resource Consumption	09-Mar-2023	4.9	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. In affected versions an already highly privileged user able to create or update Compositions can specify an arbitrarily high index in a patch's `ToFieldPath`, which could lead to excessive memory usage once such Composition is selected for a Composite resource. Compositions allow users to specify patches inserting elements into arrays at an arbitrary index. When a Composition is selected for a Composite Resource, patches are evaluated and if a specified index is greater than the current size of the target slice, Crossplane will grow that slice up to the specified index, which could lead to an excessive amount	https://github.com/crossplane/crossplane/security/advisories/GHSA-v829-x6hh-cqfq	A-CRO-CROS-280323/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of memory usage and therefore the Pod being OOM-Killed. The index is already capped to the maximum value for a uint32 (4294967295) when parsed, but that is still an unnecessarily large value. This issue has been addressed in versions 1.11.2, 1.10.3, and 1.9.2. Users are advised to upgrade. Users unable to upgrade can restrict write privileges on Compositions to only admin users as a workaround. **CVE ID : CVE-2023-27484**		
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.2					
Uncontrolled Resource Consumption	09-Mar-2023	4.9	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. In affected versions an already highly privileged user able to create or update Compositions can specify an arbitrarily high index in a patch's `ToFieldPath`, which could lead to	https://github.com/crossplane/crossplane/security/advisories/GHSA-v829-x6hh-cqfq	A-CRO-CROS-280323/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			excessive memory usage once such Composition is selected for a Composite resource. Compositions allow users to specify patches inserting elements into arrays at an arbitrary index. When a Composition is selected for a Composite Resource, patches are evaluated and if a specified index is greater than the current size of the target slice, Crossplane will grow that slice up to the specified index, which could lead to an excessive amount of memory usage and therefore the Pod being OOM-Killed. The index is already capped to the maximum value for a uint32 (4294967295) when parsed, but that is still an unnecessarily large value. This issue has been addressed in versions 1.11.2, 1.10.3, and 1.9.2. Users are advised to upgrade. Users unable to upgrade can restrict write privileges on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compositions to only admin users as a workaround. **CVE ID : CVE-2023-27484**		
Affected Version(s): From (including) 1.9.0 Up to (excluding) 1.9.2					
Uncontrolled Resource Consumption	09-Mar-2023	4.9	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. In affected versions an already highly privileged user able to create or update Compositions can specify an arbitrarily high index in a patch's `ToFieldPath`, which could lead to excessive memory usage once such Composition is selected for a Composite resource. Compositions allow users to specify patches inserting elements into arrays at an arbitrary index. When a Composition is selected for a Composite Resource, patches are evaluated and if a specified index is greater than the current size of the target slice, Crossplane will grow	https://github.com/crossplane/crossplane/security/advisories/GHSA-v829-x6hh-cqfq	A-CRO-CROS-280323/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that slice up to the specified index, which could lead to an excessive amount of memory usage and therefore the Pod being OOM-Killed. The index is already capped to the maximum value for a uint32 (4294967295) when parsed, but that is still an unnecessarily large value. This issue has been addressed in versions 1.11.2, 1.10.3, and 1.9.2. Users are advised to upgrade. Users unable to upgrade can restrict write privileges on Compositions to only admin users as a workaround. **CVE ID : CVE-2023-27484**		
Product: crossplane-runtime					
Affected Version(s): 0.16.0					
Uncontrolled Resource Consumption	09-Mar-2023	7.5	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. An out of memory panic vulnerability has been discovered in affected versions. Applications that use	https://github.com/crossplane/crossplane-runtime/commit/53508a9f4374604db140dd8ab2fa52276441e738, https://github.com/cross	A-CRO-CROS-280323/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the `Paved` type's `SetValue` method with user provided input without proper validation might use excessive amounts of memory and cause an out of memory panic. In the fieldpath package, the Paved.SetValue method sets a value on the Paved object according to the provided path, without any validation. This allows setting values in slices at any provided index, which grows the target array up to the requested index, the index is currently capped at max uint32 (4294967295) given how indexes are parsed, but that is still an unnecessarily large value. If callers are not validating paths' indexes on their own, which most probably are not going to do, given that the input is parsed directly in the SetValue method, this could allow users to consume arbitrary amounts of memory. Applications that do	plane/crossplane-runtime/security/advisories/GHSA-vfvj-3m3g-m532	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not use the `Paved` type's `SetValue` method are not affected. This issue has been addressed in versions 0.16.1 and 0.19.2. Users are advised to upgrade. Users unable to upgrade can parse and validate the path before passing it to the `SetValue` method of the `Paved` type, constraining the index size as deemed appropriate. **CVE ID : CVE-2023-27483**		
Affected Version(s): From (including) 0.19.0 Up to (excluding) 0.19.2					
Uncontrolled Resource Consumption	09-Mar-2023	7.5	crossplane-runtime is a set of go libraries used to build Kubernetes controllers in Crossplane and its related stacks. An out of memory panic vulnerability has been discovered in affected versions. Applications that use the `Paved` type's `SetValue` method with user provided input without proper validation might use excessive amounts of memory and cause an out of memory panic. In the fieldpath package,	https://github.com/crossplane/crossplane-runtime/commit/53508a9f4374604db140dd8ab2fa52276441e738, https://github.com/crossplane/crossplane-runtime/security/advisories/GHSA-vfvj-3m3g-m532	A-CRO-CROS-280323/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Paved.SetValue method sets a value on the Paved object according to the provided path, without any validation. This allows setting values in slices at any provided index, which grows the target array up to the requested index, the index is currently capped at max uint32 (4294967295) given how indexes are parsed, but that is still an unnecessarily large value. If callers are not validating paths' indexes on their own, which most probably are not going to do, given that the input is parsed directly in the SetValue method, this could allow users to consume arbitrary amounts of memory. Applications that do not use the `Paved` type's `SetValue` method are not affected. This issue has been addressed in versions 0.16.1 and 0.19.2. Users are advised to upgrade. Users unable to upgrade can parse		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and validate the path before passing it to the `SetValue` method of the `Paved` type, constraining the index size as deemed appropriate. **CVE ID : CVE-2023-27483**		
Vendor: dash7-alliance					
Product: dash7_alliance_protcol					
Affected Version(s): * Up to (including) 0.5.0					
Out-of-bounds Write	01-Mar-2023	8.1	The Sub-IoT implementation of the DASH 7 Alliance protocol has a vulnerability that can lead to an out-of-bounds write prior to implementation version 0.5.0. If the protocol has been compiled using default settings, this will only grant the attacker access to allocated but unused memory. However, if it was configured using non-default settings, there is the possibility that exploiting this vulnerability could lead to system crashes and remote code execution. **CVE ID : CVE-2023-0847**	https://github.com/Sub-IoT/Sub-IoT-Stack/security/advisories/GHSA-ggxh-88wc-c4fg	A-DAS-DASH-280323/175
Vendor: dataiku					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: data_science_studio					
Affected Version(s): * Up to (excluding) 11.3.2					
Unrestricted Upload of File with Dangerous Type	01-Mar-2023	6.5	In Dataiku DSS 11.2.1, an attacker can download other Dataiku files that were uploaded to the myfiles section by specifying the target username in a download request. **CVE ID : CVE-2023-24045**	N/A	A-DAT-DATA-280323/176
Vendor: Debian					
Product: debmany					
Affected Version(s): 0.88.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Mar-2023	7.8	debmany in debian-goodies 0.88.1 allows attackers to execute arbitrary shell commands (because of an eval call) via a crafted .deb file. (The path is shown to the user before execution.) **CVE ID : CVE-2023-27635**	https://bugs.debian.org/1031267	A-DEB-DEBM-280323/177
Vendor: Dell					
Product: emc_networker					
Affected Version(s): * Up to (excluding) 19.6					
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	Dell NetWorker versions 19.5 and earlier contain 'RabbitMQ' version disclosure vulnerability. A NetWorker server user with remote	https://www.dell.com/support/kbdoc/en-us/000210471/dsa-2023-058-dell-	A-DEL-EMC_-280323/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to NetWorker clients may potentially exploit this vulnerability and may launch target-specific attacks. **CVE ID : CVE-2023-24567**	networker-security-update-for-version-disclosure-vulnerability	
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	Dell NetWorker versions 19.5 and earlier contain 'Apache Tomcat' version disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially exploit this vulnerability and may launch target-specific attacks. **CVE ID : CVE-2023-25544**	https://www.dell.com/support/kbdoc/en-us/000210471/dsa-2023-058-dell-networker-security-update-for-version-disclosure-vulnerability	A-DEL-EMC_-280323/179
Product: powerscale_onefs					
Affected Version(s): From (including) 9.4.0.0 Up to (including) 9.4.0.11					
Exposure of Resource to Wrong Sphere	02-Mar-2023	6.7	Dell PowerScale OneFS 9.4.0.x contains exposure of sensitive information to an unauthorized actor. A malicious authenticated local user could potentially exploit this vulnerability in certificate management, leading to a potential system takeover.	https://www.dell.com/support/kbdoc/en-us/000209895/dell-emc-powerscale-onefs-security-updates-for-multiple-security	A-DEL-POWE-280323/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25536		
Vendor: design_and_implementation_of_covid-19_directory_on_vaccination_system_project					
Product: design_and_implementation_of_covid-19_directory_on_vaccination_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0. This issue affects some unknown processing of the file /admin/login.php. The manipulation of the argument txtusername/txtpassword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222851. **CVE ID : CVE-2023-1352**	N/A	A-DES-DESI-280323/181
Improper Neutralization of Input During Web Page Generation	11-Mar-2023	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Design and Implementation of	N/A	A-DES-DESI-280323/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Covid-19 Directory on Vaccination System 1.0. Affected is an unknown function of the file verification.php. The manipulation of the argument txtvaccinationID leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222852. **CVE ID : CVE-2023-1353**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Mar-2023	6.1	A vulnerability has been found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file register.php. The manipulation of the argument txtfullname/txtage/txtaddress/txtphone leads to cross site scripting. The attack can be launched	N/A	A-DES-DESI-280323/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222853 was assigned to this vulnerability. **CVE ID : CVE-2023-1354**		
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2022.3.13					
N/A	10-Mar-2023	6.5	Improper access control in the secure messages feature in Devolutions Server 2022.3.12 and below allows an authenticated attacker that possesses the message UUID to access the data it contains. **CVE ID : CVE-2023-1201**	https://devolutions.net/security/advisories/DEVO-2023-0005	A-DEV-DEVO-280323/184
Affected Version(s): * Up to (including) 2022.3.12					
N/A	01-Mar-2023	8.8	Improper access controls on some API endpoints in Devolutions Server 2022.3.12 and earlier could allow a standard privileged user to perform privileged actions. **CVE ID : CVE-2023-0951**	https://devolutions.net/security/advisories/DEVO-2023-0003	A-DEV-DEVO-280323/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Mar-2023	8.8	Insufficient input sanitization in the documentation feature of Devolutions Server 2022.3.12 and earlier allows an authenticated attacker to perform an SQL Injection, potentially resulting in unauthorized access to system resources. **CVE ID : CVE-2023-0953**	https://devolutions.net/security/advisories/DEVO-2023-0003	A-DEV-DEVO-280323/186
Incorrect Authorization	01-Mar-2023	6.5	Improper access controls on entries in Devolutions Server 2022.3.12 and earlier could allow an authenticated user to access sensitive data without proper authorization. **CVE ID : CVE-2023-0952**	https://devolutions.net/security/advisories/DEVO-2023-0003	A-DEV-DEVO-280323/187
Product: remote_desktop_manager					
Affected Version(s): * Up to (excluding) 2022.3.1.6					
N/A	10-Mar-2023	6.5	Improper removal of sensitive data in the entry edit feature of Hub Business submodule in Devolutions Remote Desktop Manager PowerShell Module 2022.3.1.5 and earlier allows an authenticated user to access sensitive data	https://devolutions.net/security/advisories/DEVO-2023-0004	A-DEV-REMO-280323/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on entries that were edited using the affected submodule. **CVE ID : CVE-2023-1203**		
Vendor: dfactory					
Product: download_attachments					
Affected Version(s): * Up to (excluding) 1.2.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The Download Attachments WordPress plugin through 1.2.24 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0076**	N/A	A-DFA-DOWN-280323/189
Vendor: discourse					
Product: discourse					
Affected Version(s): * Up to (excluding) 3.1.0					
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-2023	5.3	Discourse is an open source platform for community discussion. Tags that are normally private are showing in metadata. This affects any site running the `tests-passed` or `beta` branches >=	https://github.com/discourse/discourse/commit/a9f2c6db64e7d78b8e0f55e7bd77c5fe3459b831	A-DIS-DISC-280323/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1.0.beta2. The issue is patched in the latest `beta` and `tests-passed` version of Discourse. **CVE ID : CVE-2023-25819**		
Affected Version(s): 3.1.0					
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-2023	5.3	Discourse is an open source platform for community discussion. Tags that are normally private are showing in metadata. This affects any site running the `tests-passed` or `beta` branches >= 3.1.0.beta2. The issue is patched in the latest `beta` and `tests-passed` version of Discourse. **CVE ID : CVE-2023-25819**	https://github.com/discourse/discourse/commit/a9f2c6db64e7d78b8e0f55e7bd77c5fe3459b831	A-DIS-DISC-280323/191
Product: discourse_yearly_review					
Affected Version(s): * Up to (excluding) 0.2					
N/A	06-Mar-2023	5.3	discourse-yearly-review is a discourse plugin which publishes an automated Year in Review topic. In affected versions a user present in a yearly review topic that is then anonymised will still have some data linked to its original account. This issue	https://github.com/discourse/discourse-yearly-review/commit/b3ab33bbf7130fca54764cf0336395a8a1eeaf3c, https://github.com/discourse/discourse-yearly-	A-DIS-DISC-280323/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been patched in commit `b3ab33bbf7` which is included in the latest version of the Discourse Yearly Review plugin. Users are advised to upgrade. Users unable to upgrade may disable the `yearly_review_enabled` setting to fully mitigate the issue. Also, it's possible to edit the anonymised user's old data in the yearly review topics manually. **CVE ID : CVE-2023-25169**	review/security/advisories/GHSA-x2r8-v85c-x3x7	
Vendor: Docker					
Product: docker_desktop					
Affected Version(s): * Up to (excluding) 4.17.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	7.8	Docker Desktop before 4.17.0 allows an attacker to execute an arbitrary command inside a Dev Environments container during initialization by tricking a user to open a crafted malicious docker-desktop:// URL. **CVE ID : CVE-2023-0628**	N/A	A-DOC-DOCK-280323/193
Affected Version(s): From (including) 4.13.0 Up to (excluding) 4.17.0					
N/A	13-Mar-2023	7.1	Docker Desktop before 4.17.0 allows	N/A	A-DOC-DOCK-280323/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions by setting the Docker host to docker.raw.sock, or npipe:////.pipe/docker_engine_linux on Windows, via the -H (--host) CLI flag or the DOCKER_HOST environment variable and launch containers without the additional hardening features provided by ECI. This would not affect already running containers, nor containers launched through the usual approach (without Docker's raw socket). The affected functionality is available for Docker Business customers only and assumes an environment where users are not granted local root or Administrator privileges. This issue has been fixed in Docker Desktop 4.17.0. Affected Docker Desktop versions: from 4.13.0 before 4.17.0. **CVE ID : CVE-2023-0629**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: dos-osaka					
Product: rakuraku_pc_cloud_agent					
Affected Version(s): * Up to (including) 2.1.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Mar-2023	9.8	Path traversal vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to upload a specially crafted file to an arbitrary directory. As a result of exploiting this vulnerability with CVE-2023-22335 and CVE-2023-22344 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device. **CVE ID : CVE-2023-22336**	https://www.dos-osaka.co.jp/news/2023/03/230301.html	A-DOS-RAKU-280323/195
Use of Hard-coded Credentials	06-Mar-2023	9.8	Use of hard-coded credentials vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to obtain the password of the debug tool and	https://www.dos-osaka.co.jp/news/2023/03/230301.html	A-DOS-RAKU-280323/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute it. As a result of exploiting this vulnerability with CVE-2023-22335 and CVE-2023-22336 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device. **CVE ID : CVE-2023-22344**		
N/A	06-Mar-2023	7.5	Improper access control vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to bypass access restriction and download an arbitrary file of the directory where the product runs. As a result of exploiting this vulnerability with CVE-2023-22336 and CVE-2023-22344 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM	https://www.dos-osaka.co.jp/news/2023/03/230301.html	A-DOS-RAKU-280323/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges by sending a specially crafted script to the affected device. **CVE ID : CVE-2023-22335**		
Product: ss1					
Affected Version(s): * Up to (including) 13.0.0.40					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Mar-2023	9.8	Path traversal vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to upload a specially crafted file to an arbitrary directory. As a result of exploiting this vulnerability with CVE-2023-22335 and CVE-2023-22344 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device. **CVE ID : CVE-2023-22336**	https://www.dos-osaka.co.jp/news/2023/03/230301.html	A-DOS-SS1-280323/198
Use of Hard-coded Credentials	06-Mar-2023	9.8	Use of hard-coded credentials vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent	https://www.dos-osaka.co.jp/news/2023/03/230301.html	A-DOS-SS1-280323/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver.2.1.8 and earlier allows a remote attacker to obtain the password of the debug tool and execute it. As a result of exploiting this vulnerability with CVE-2023-22335 and CVE-2023-22336 vulnerabilities together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device. **CVE ID : CVE-2023-22344**		
N/A	06-Mar-2023	7.5	Improper access control vulnerability in SS1 Ver.13.0.0.40 and earlier and Rakuraku PC Cloud Agent Ver.2.1.8 and earlier allows a remote attacker to bypass access restriction and download an arbitrary file of the directory where the product runs. As a result of exploiting this vulnerability with CVE-2023-22336 and CVE-2023-22344 vulnerabilities	https://www.dos-osaka.co.jp/news/2023/03/230301.html	A-DOS-SS1-280323/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			together, it may allow a remote attacker to execute an arbitrary code with SYSTEM privileges by sending a specially crafted script to the affected device. **CVE ID : CVE-2023-22335**		
Vendor: dot-lens_project					
Product: dot-lens					
Affected Version(s): * Up to (including) 1.2.3					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	06-Mar-2023	7.5	All versions of the package dot-lens are vulnerable to Prototype Pollution via the set() function in index.js file. **CVE ID : CVE-2023-26106**	N/A	A-DOT-DOT--280323/201
Vendor: drag_and_drop_multiple_file_uploader_pro_-_contact_form_7_project					
Product: drag_and_drop_multiple_file_uploader_pro_-_contact_form_7					
Affected Version(s): 5.0.6.1					
Relative Path Traversal	01-Mar-2023	9.8	A vulnerability was found in Drag and Drop Multiple File Upload Contact Form 7 5.0.6.1. It has been classified as critical. Affected is an unknown function of the file admin-ajax.php. The manipulation of the argument upload_name leads to relative path traversal. It is possible to launch	N/A	A-DRA-DRAG-280323/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222072. **CVE ID : CVE-2023-1112**		
Vendor: eaglevisionit					
Product: evision_responsive_column_layout_shortcodes					
Affected Version(s): * Up to (excluding) 2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The eVision Responsive Column Layout Shortcodes WordPress plugin through 2.3 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0064**	N/A	A-EAG-EVIS-280323/203
Vendor: easyappointments					
Product: easyappointments					
Affected Version(s): * Up to (excluding) 1.5.0					
Use of Hard-coded Credentials	08-Mar-2023	9.8	Use of Hard-coded Credentials in GitHub repository alextselegidis/easya	https://huntr.dev/bounties/91c31eb6-024d-4ad3-88fe-f15b03fd20f	A-EAS-EASY-280323/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ppointments prior to 1.5.0. **CVE ID : CVE-2023-1269**	5, https://github.com/alextselegidis/easyappointments/commit/2731d2f17c5140c562426b857e9f5d63da5c4593	
Improper Control of Generation of Code ('Code Injection')	13-Mar-2023	3.8	Code Injection in GitHub repository alextselegidis/easyappointments prior to 1.5.0. **CVE ID : CVE-2023-1367**	https://hunt r.dev/bounties/16bc74e2-1825-451f-bff7-bfdc1ea75cc2, https://github.com/alextselegidis/easyappointments/commit/453c6e130229718680c91bef450db643a0f263e4	A-EAS-EASY-280323/205
Vendor: easyimages2.0_project					
Product: easyimages2.0					
Affected Version(s): * Up to (excluding) 2.6.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository icret/easyimages2.0 prior to 2.6.7. **CVE ID : CVE-2023-1181**	https://hunt r.dev/bounties/f5cb8816-fc12-4282-9571-81f25670e04a, https://github.com/icret/easyimages2.0/commit/95a6caf1c660a7342a8f11	A-EAS-EASY-280323/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				d70c2dbf7ebcbe2966	
Vendor: Ebay					
Product: sketchsvg					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	06-Mar-2023	7.8	All versions of the package sketchsvg are vulnerable to Arbitrary Code Injection when invoking shell.exec without sanitization nor parametrization while concatenating the current directory as part of the command string. **CVE ID : CVE-2023-26107**	N/A	A-EBA-SKET-280323/207
Vendor: Ec-cube					
Product: ec-cube					
Affected Version(s): 3.0.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**		
Affected Version(s): 4.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/209
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Product List Screen and Product Detail Screen of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to inject an arbitrary script. **CVE ID : CVE-2023-22838**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Authentication Key Settings of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-25077**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/211
Affected Version(s): 4.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script.	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22438		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Product List Screen and Product Detail Screen of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22838**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Authentication Key Settings of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-25077**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/214
Affected Version(s): 4.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://ww	A-EC--EC-C-280323/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	w.ec-cube.net/info/weakness/20230214/index_2.php	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Product List Screen and Product Detail Screen of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22838**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/216
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Authentication Key Settings of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-25077**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/217
Affected Version(s): From (including) 2.11.0 Up to (including) 2.11.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/218
Affected Version(s): From (including) 2.12.0 Up to (including) 2.12.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**		
Affected Version(s): From (including) 2.13.0 Up to (including) 2.13.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/220
Affected Version(s): From (including) 2.17.0 Up to (including) 2.17.2					
Improper Neutralization of Input During Web Page Generation	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://ww	A-EC--EC-C-280323/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	w.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	
Affected Version(s): From (including) 3.0.0 Up to (including) 3.0.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script.	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22438		
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/223
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Product List Screen and Product Detail Screen of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22838**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Authentication Key Settings of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-25077**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/225
Affected Version(s): From (including) 4.1.0 Up to (including) 4.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Contents Management of EC-CUBE 4 series (EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0), EC-CUBE 3 series (EC-CUBE 3.0.0 to 3.0.18-p5), and EC-CUBE 2 series (EC-CUBE 2.11.0 to 2.11.5, EC-CUBE 2.12.0 to 2.12.6, EC-CUBE 2.13.0 to 2.13.5, and EC-CUBE 2.17.0 to 2.17.2) allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22438**	https://www.ec-cube.net/info/weakness/20230214/index_3.php, https://www.ec-cube.net/info/weakness/20230214/, https://www.ec-cube.net/info/weakness/20230214/index_2.php	A-EC--EC-C-280323/226
Improper Neutralization of	06-Mar-2023	5.4	Cross-site scripting vulnerability in Product List Screen	https://www.ec-cube.net/inf	A-EC--EC-C-280323/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			and Product Detail Screen of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-22838**	o/weakness/20230214/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Cross-site scripting vulnerability in Authentication Key Settings of EC-CUBE 4.0.0 to 4.0.6-p2, EC-CUBE 4.1.0 to 4.1.2-p1, and EC-CUBE 4.2.0 allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-25077**	https://www.ec-cube.net/info/weakness/20230214/	A-EC--EC-C-280323/228
Vendor: Eclipse					
Product: business_intelligence_and_reporting_tools					
Affected Version(s): From (including) 2.6.2 Up to (excluding) 4.13.0					
N/A	15-Mar-2023	8.8	In Eclipse BIRT, starting from version 2.6.2, the default configuration allowed to retrieve a report from the same host using an absolute HTTP path for the report parameter (e.g. __report=http://xyz.com/report.rptdesign). If the host indicated in the __report parameter	https://bugs.eclipse.org/bugs/show_bug.cgi?id=580391	A-ECL-BUSI-280323/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			matched the HTTP Host header value, the report would be retrieved. However, the Host header can be tampered with on some configurations where no virtual hosts are put in place (e.g. in the default configuration of Apache Tomcat) or when the default host points to the BIRT server. This vulnerability was patched on Eclipse BIRT 4.13. **CVE ID : CVE-2023-0100**		
Vendor: ehuacui-bbs_project					
Product: ehuacui-bbs					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	A vulnerability was found in ehuacui bbs. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore,	N/A	A-EHU-EHUA-280323/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-222388. **CVE ID : CVE-2023-1200**		
Vendor: electronic_medical_records_system_project					
Product: electronic_medical_records_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Mar-2023	9.8	A vulnerability was found in SourceCodester Electronic Medical Records System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file administrator.php of the component Cookie Handler. The manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222163. **CVE ID : CVE-2023-1151**	N/A	A-ELE-ELEC-280323/231
Vendor: elf-parser_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: elf-parser					
Affected Version(s): -					
Improper Resource Shutdown or Release	02-Mar-2023	5.5	A vulnerability, which was classified as problematic, was found in finixbit elf-parser. Affected is the function elf_parser::Elf_parser ::get_segments of the file elf_parser.cpp. The manipulation leads to denial of service. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. VDB-222222 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1157**	N/A	A-ELF-ELF--280323/232
Vendor: employee_payslip_generator_system_project					
Product: employee_payslip_generator_system					
Affected Version(s): 1.2.0					
Improper Neutralization of Special Elements used in an	12-Mar-2023	4.9	A vulnerability was found in SourceCodester Employee Payslip Generator with Sending Mail 1.2.0	N/A	A-EMP-EMPL-280323/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			and classified as critical. This issue affects some unknown processing of the file classes/Users.php?f=save of the component New User Creation. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222863. **CVE ID : CVE-2023-1360**		
Vendor: enhancesoft					
Product: osticket					
Affected Version(s): * Up to (excluding) 1.16.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	6.1	Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6. **CVE ID : CVE-2023-1320**	https://hunter.dev/bounties/c2bb34ac-452d-4624-a1b9-c5b54f52f0cd, https://github.com/osticket/osticket/commit/86f9693dc64ed54220ed6c10e13e824ca4f6aacf	A-ENH-OSTI-280323/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository osticket/osticket prior to v1.16.6. **CVE ID : CVE-2023-1315**	https://github.com/osticket/osticket/commit/ec6043935b4e30b5c0dfa544e2567171828 08a2e, https://hunt r.dev/bounties/70a7fd8c-7e6f-4a43-9f8c-163b8967b16e	A-ENH-OSTI-280323/235
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6. **CVE ID : CVE-2023-1316**	https://hunt r.dev/bounties/c6353bab-c382-47f6-937b-56d253f2e8d3, https://github.com/osticket/osticket/commit/091ddba965132d26bdbeb004fcc44bd8fd056b71	A-ENH-OSTI-280323/236
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository osticket/osticket prior to v1.16.6. **CVE ID : CVE-2023-1317**	https://hunt r.dev/bounties/c3e27af2-358b-490b-9baf-e451663e4e5f, https://github.com/osticket/osticket/commit/daee20fdd8ac926d9aee700b2	A-ENH-OSTI-280323/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				01ac2cb35d448ca	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository osticket/osticket prior to v1.16.6. **CVE ID : CVE-2023-1318**	https://github.com/osticket/osticket/commit/343a2b47e164dd9090a3c9477ef273f0efa16a7d, https://hunt r.dev/bounties/e58b38e0-4897-4bb0-84e8-a7ad8efab338	A-ENH-OSTI-280323/238
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository osticket/osticket prior to v1.16.6. **CVE ID : CVE-2023-1319**	https://github.com/osticket/osticket/commit/9fb01bc12fbae06aa2c2b4d1bc9b4a08db4bb3e0, https://hunt r.dev/bounties/a822067a-d90d-4c3e-b9ef-9b2a5c2bc97f	A-ENH-OSTI-280323/239
Vendor: eskom					
Product: e-belediye					
Affected Version(s): From (including) 1.0.0.95 Up to (excluding) 1.0.0.100					
Missing Authorization	01-Mar-2023	9.8	Improper Input Validation, Missing Authorization vulnerability in Eskom Bilgisayar e-Belediye allows Information	N/A	A-ESK-E-BE-280323/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elicitation.This issue affects e-Belediye: from 1.0.0.95 before 1.0.0.100. **CVE ID : CVE-2023-1114**		
Vendor: fabulatech					
Product: webcam_for_remote_desktop					
Affected Version(s): 2.8.42					
NULL Pointer Dereference	06-Mar-2023	5.5	A vulnerability has been found in FabulaTech Webcam for Remote Desktop 2.8.42 and classified as problematic. This vulnerability affects unknown code in the library ftwebcam.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-222358 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1186**	N/A	A-FAB-WEBC-280323/241
Improper Resource Shutdown or Release	06-Mar-2023	5.5	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42 and classified as problematic. This issue affects some	N/A	A-FAB-WEBC-280323/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown processing in the library ftwebcam.sys of the component Global Variable Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222359. **CVE ID : CVE-2023-1187**		
Improper Resource Shutdown or Release	06-Mar-2023	5.5	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42. It has been classified as problematic. Affected is an unknown function in the library ftwebcam.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222360.	N/A	A-FAB-WEBC-280323/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1188		
Vendor: feiqu-opensource_project					
Product: feiqu-opensource					
Affected Version(s): -					
N/A	08-Mar-2023	8.8	feiqu-opensource Background Vertical authorization vulnerability exists in IndexController.java. demo users with low permission can perform operations within the permission of the admin super administrator and can use this vulnerability to change the blacklist IP address in the system at will. **CVE ID : CVE-2023-27088**	N/A	A-FEI-FEIQ-280323/244
Vendor: file_tracker_manager_system_project					
Product: file_tracker_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	A vulnerability was found in SourceCodester File Tracker Manager System 1.0. It has been classified as critical. Affected is an unknown function of the file /file_manager/login.php of the component POST Parameter Handler.	https://github.com/godownio/bug_report/blob/main/vendors/hemedy99/File%20Tracker%20Manager%20System/SQLi-1.md	A-FIL-FILE-280323/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222648. **CVE ID : CVE-2023-1294**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester File Tracker Manager System 1.0. This affects an unknown part of the file normal/borrow1.php. The manipulation of the argument id with the input 1"><script>alert(1111)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222663. **CVE ID : CVE-2023-1302**	N/A	A-FIL-FILE-280323/246
Vendor: flarum					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: flarum					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Mar-2023	4.9	flarum is a forum software package for building communities. In versions prior to 1.7.0 an admin account which has already been compromised by an attacker may use a vulnerability in the `LESS` parser which can be exploited to read sensitive files on the server through the use of path traversal techniques. An attacker can achieve this by providing an absolute path to a sensitive file in the custom `LESS` setting, which the `LESS` parser will then read. For example, an attacker could use the following code to read the contents of the `/etc/passwd` file on a linux machine. The scope of what files are vulnerable will depend on the permissions given to the running flarum process. The vulnerability has been addressed in	https://github.com/flarum/framework/security/advisories/GHSA-vhm8-wwrf-3gcw, https://github.com/flarum/framework/commit/1761660c98ea5a3e9665fb8e6041d1f2ee62a444	A-FLA-FLAR-280323/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version `1.7`. Users should upgrade to this version to mitigate the vulnerability. Users unable to upgrade may mitigate the vulnerability by ensuring that their admin accounts are secured with strong passwords and follow other best practices for account security. Additionally, users can limit the exposure of sensitive files on the server by implementing appropriate file permissions and access controls at the operating system level. **CVE ID : CVE-2023-27577**		
Vendor: Flatpress					
Product: flatpress					
Affected Version(s): * Up to (excluding) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1106**	https://hunter.dev/bounties/1288ec00-f69d-4b84-abce-efc9a97941a0, https://github.com/flatpressblog/flatpress/commit/5f23b4c2ea	A-FLA-FLAT-280323/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				c294cc0ba5e541f83a6f8a26f9fed1	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1103**	https://github.com/flatpressblog/flatpress/commit/3cc223dec5260e533a84b5cf5780d3a4fbf21241, https://hunt r.dev/bounties/4c5a8af6-3078-4180-bb30-33b57a5540e6	A-FLA-FLAT-280323/249
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1104**	https://hunt r.dev/bounties/a4909b4e-ab3c-41d6-b0d8-1c6e933bf758, https://github.com/flatpressblog/flatpress/commit/f6394eac7a0e001d2b1ac638d3313e531d19ea93	A-FLA-FLAT-280323/250
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1107**	https://github.com/flatpressblog/flatpress/commit/d3f329496536dc99f9707f2f295d571d65a496f5, https://hunt r.dev/bounti	A-FLA-FLAT-280323/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				es/4b880868-bd28-4fd0-af56-7686e55d3762	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1146**	https://hunter.dev/bounties/d6d1e1e2-2f67-4d28-aa84-b30fb1d2e737, https://github.com/flatpressblog/flatpress/commit/0ee4f2e8a7b9276880b56858e408cc9c6643cc3b	A-FLA-FLAT-280323/252
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1147**	https://hunter.dev/bounties/187f5353-f866-4d26-a5ba-fca378520020, https://github.com/flatpressblog/flatpress/commit/264217f318a8852c4f3e34350d4a0e1363cdd727	A-FLA-FLAT-280323/253
Improper Neutralization of Input During Web Page Generation	02-Mar-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2023-1148**	https://github.com/flatpressblog/flatpress/commit/3a32aad0dec5df24c6576d7567d4f2eadbfc75de,	A-FLA-FLAT-280323/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				https://hunt r.dev/bounti es/f0cc2c4b-fdf9-483b-9a83-4e0dfeb4dac 7	
Affected Version(s): * Up to (excluding) 2022-12-25					
External Control of File Name or Path	01-Mar-2023	8.1	External Control of File Name or Path in GitHub repository flatpressblog/flatpre ss prior to 1.3. **CVE ID : CVE-2023-1105**	https://hunt r.dev/bounti es/4089a63f -cffd-42f3-b8d8-e80b6bd9c8 0f, https://githu b.com/flatpr essblog/flatp ress/commit /5d5c7f6d8f 072d14926f c2c3a97cdd 763802f170	A-FLA-FLAT-280323/255
Vendor: Fortinet					
Product: fortianalyzer					
Affected Version(s): From (including) 6.4.0 Up to (excluding) 6.4.11					
Cleartext Storage of Sensitive Informatio n	07-Mar-2023	3.1	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiAnalyzer versions 7.2.0 through 7.2.1, 7.0.0 through 7.0.4 and 6.4.0 through 6.4.10 may allow a remote authenticated attacker to read the client machine password in plain text in a heartbeat	https://forti guard.com/p sirt/FG-IR-22-447	A-FOR-FORT-280323/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			response when a log-fetch request is made from the FortiAnalyzer **CVE ID : CVE-2023-23776**		
Affected Version(s): From (including) 6.4.0 Up to (excluding) 7.0.6					
Improper Neutralization of Formula Elements in a CSV File	07-Mar-2023	7.3	A improper neutralization of formula elements in a CSV file vulnerability in Fortinet FortiAnalyzer 6.4.0 - 6.4.9, 7.0.0 - 7.0.5, and 7.2.0 - 7.2.1 allows local attacker to execute unauthorized code or commands via inserting spreadsheet formulas in macro names. **CVE ID : CVE-2023-25611**	https://fortiguard.com/psirt/FG-IR-22-488	A-FOR-FORT-280323/257
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.5					
Cleartext Storage of Sensitive Information	07-Mar-2023	3.1	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiAnalyzer versions 7.2.0 through 7.2.1, 7.0.0 through 7.0.4 and 6.4.0 through 6.4.10 may allow a remote authenticated attacker to read the client machine password in plain	https://fortiguard.com/psirt/FG-IR-22-447	A-FOR-FORT-280323/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			text in a heartbeat response when a log-fetch request is made from the FortiAnalyzer **CVE ID : CVE-2023-23776**		
Affected Version(s): From (including) 7.2.0 Up to (excluding) 7.2.2					
Improper Neutralization of Formula Elements in a CSV File	07-Mar-2023	7.3	A improper neutralization of formula elements in a CSV file vulnerability in Fortinet FortiAnalyzer 6.4.0 - 6.4.9, 7.0.0 - 7.0.5, and 7.2.0 - 7.2.1 allows local attacker to execute unauthorized code or commands via inserting spreadsheet formulas in macro names. **CVE ID : CVE-2023-25611**	https://fortiguard.com/psirt/FG-IR-22-488	A-FOR-FORT-280323/259
Cleartext Storage of Sensitive Information	07-Mar-2023	3.1	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiAnalyzer versions 7.2.0 through 7.2.1, 7.0.0 through 7.0.4 and 6.4.0 through 6.4.10 may allow a remote authenticated attacker to read the client machine password in plain	https://fortiguard.com/psirt/FG-IR-22-447	A-FOR-FORT-280323/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			text in a heartbeat response when a log-fetch request is made from the FortiAnalyzer **CVE ID : CVE-2023-23776**		
Product: fortiauthenticator					
Affected Version(s): From (including) 5.4.0 Up to (excluding) 6.5.0					
Improper Restriction of Excessive Authentication Attempts	09-Mar-2023	5.3	A improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiAuthenticator 6.4.x and before allows a remote unauthenticated attacker to partially exhaust CPU and memory via sending numerous HTTP requests to the login form. **CVE ID : CVE-2023-26208**	https://fortiguard.com/psirt/FG-IR-20-078	A-FOR-FORT-280323/261
Product: fortideceptor					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 3.2.0					
Improper Restriction of Excessive Authentication Attempts	09-Mar-2023	5.3	A improper restriction of excessive authentication attempts vulnerability [CWE-307] in Fortinet FortiDeceptor 3.1.x and before allows a remote unauthenticated	https://fortiguard.com/psirt/FG-IR-20-078	A-FOR-FORT-280323/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to partially exhaust CPU and memory via sending numerous HTTP requests to the login form. **CVE ID : CVE-2023-26209**		
Product: fortisoar					
Affected Version(s): From (including) 7.3.0 Up to (excluding) 7.3.2					
N/A	07-Mar-2023	7.2	A improper access control vulnerability in Fortinet FortiSOAR 7.3.0 - 7.3.1 allows an attacker authenticated on the administrative interface to perform unauthorized actions via crafted HTTP requests. **CVE ID : CVE-2023-25605**	https://fortiguard.com/psirt/FG-IR-23-050	A-FOR-FORT-280323/263
Vendor: freshrss					
Product: freshrss					
Affected Version(s): From (including) 1.9.0 Up to (excluding) 1.21.0					
Insertion of Sensitive Information into Log File	06-Mar-2023	5.5	FreshRSS is a self-hosted RSS feed aggregator. When using the greader API, the provided password is logged in clear in `users/_/log_api.txt` in the case where the authentication fails. The issues occurs in `authorizationToUser()` in `greader.php`. If there is an issue	https://github.com/FreshRSS/FreshRSS/security/advisories/GHSA-8vvv-jxg6-8578, https://github.com/FreshRSS/FreshRSS/commit/075cf4c800063e3cc65c3d	A-FRE-FRES-280323/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the request or the credentials, `unauthorized()` or `badRequest()` is called. Both these functions are printing the return of `debugInfo()` in the logs. `debugInfo()` will return the content of the request. By default, this will be saved in `users/_/log_api.txt` and if the const `COPY_LOG_TO_SYSLOG` is true, in syslogs as well. Exploiting this issue requires having access to logs produced by FreshRSS. Using the information from the logs, a malicious individual could get users' API keys (would be displayed if the users fills in a bad username) or passwords. **CVE ID : CVE-2023-22481**	41a9c23222e8ebb554	
Vendor: friendly_island_pizza_website_and_ordering_system_project					
Product: friendly_island_pizza_website_and_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	09-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Friendly Island Pizza Website and	N/A	A-FRI-FRIE-280323/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			Ordering System 1.0. Affected by this issue is some unknown functionality of the file deleteorder.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222662 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1301**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This affects an unknown part of the file large.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-FRI-FRIE-280323/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			associated identifier of this vulnerability is VDB-222699. **CVE ID : CVE-2023-1311**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This vulnerability affects unknown code of the file paypalsuccess.php of the component POST Parameter Handler. The manipulation of the argument cusid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222904. **CVE ID : CVE-2023-1378**	N/A	A-FRI-FRIE-280323/267
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Mar-2023	9.8	A vulnerability was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file addmem.php of the	https://github.com/AureliusLia/bug_report/blob/main/vendors/Skynidnine/Friendly%20Island%20Pizza%20Website%20and%20Ordering%20Syste	A-FRI-FRIE-280323/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component POST Parameter Handler. The manipulation of the argument firstname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223127. **CVE ID : CVE-2023-1379**	m/SQLi-1.md	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Mar-2023	6.1	A vulnerability classified as problematic was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file cashconfirm.php of the component POST Parameter Handler. The manipulation of the argument transactioncode leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-	https://github.com/2889436547/bug_report/blob/main/vendors/Skynidnine/Friendly%20Island%20Pizza%20Website%20and%20Ordering%20System/XSS-1.md	A-FRI-FRIE-280323/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			223129 was assigned to this vulnerability. **CVE ID : CVE-2023-1418**		
Vendor: Froxlor					
Product: froxlor					
Affected Version(s): * Up to (excluding) 2.0.13					
Authentication Bypass by Primary Weakness	10-Mar-2023	9.8	Authentication Bypass by Primary Weakness in GitHub repository froxlor/froxlor prior to 2.0.13. **CVE ID : CVE-2023-1307**	https://github.com/froxlor/froxlor/commit/6777fbf229200f4fd566022e186548391219ab23, https://hunt r.dev/bounties/5fe85af4-a667-41a9-a00d-f99e07c5e2f1	A-FRO-FROX-280323/270
Vendor: fullworksplugins					
Product: quick_event_manager					
Affected Version(s): * Up to (excluding) 9.7.5					
Cross-Site Request Forgery (CSRF)	01-Mar-2023	5.4	Cross-Site Request Forgery (CSRF) vulnerability in Fullworks Quick Event Manager plugin <= 9.7.4 affecting all registration actions (delete, delete all, edit, update). **CVE ID : CVE-2023-23974**	N/A	A-FUL-QUIC-280323/271
Vendor: funadmin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: funadmin					
Affected Version(s): 3.2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/database/list. **CVE ID : CVE-2023-24773**	N/A	A-FUN-FUNA-280323/272
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the selectFields parameter at \controller\auth\Auth.php. **CVE ID : CVE-2023-24774**	https://github.com/funadmin/funadmin/issues/12	A-FUN-FUNA-280323/273
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the selectFields parameter at \member\Member.php. **CVE ID : CVE-2023-24775**	N/A	A-FUN-FUNA-280323/274
N/A	06-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a remote code execution (RCE) vulnerability via the component	N/A	A-FUN-FUNA-280323/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			\controller\Addon.php. **CVE ID : CVE-2023-24776**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/table/list. **CVE ID : CVE-2023-24777**	N/A	A-FUN-FUNA-280323/276
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at /databases/table/columns. **CVE ID : CVE-2023-24780**	N/A	A-FUN-FUNA-280323/277
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the selectFields parameter at \member\MemberLevel.php. **CVE ID : CVE-2023-24781**	N/A	A-FUN-FUNA-280323/278
Improper Neutralization of Special Elements used in an	08-Mar-2023	9.8	Funadmin v3.2.0 was discovered to contain a SQL injection vulnerability via the id parameter at	N/A	A-FUN-FUNA-280323/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			/databases/database/edit. **CVE ID : CVE-2023-24782**		
Vendor: gadget_works_online_ordering_system_project					
Product: gadget_works_online_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Gadget Works Online Ordering System 1.0. This affects an unknown part of the file /philosophy/admin/login.php of the component POST Parameter Handler. The manipulation of the argument user_email 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 identifier VDB-222861 was assigned to this vulnerability. **CVE ID : CVE-2023-1358**	N/A	A-GAD-GADG-280323/280
Improper Neutralization of Input During Web Page Generation	12-Mar-2023	4.8	A vulnerability has been found in SourceCodester Gadget Works Online Ordering System 1.0 and classified as problematic. This	N/A	A-GAD-GADG-280323/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability affects unknown code of the file /philosophy/admin/user/controller.php?action=add of the component Add New User. The manipulation of the argument U_NAME leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222862 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1359**		
Vendor: ghost					
Product: ghost					
Affected Version(s): 5.35.0					
Missing Authorization	05-Mar-2023	5.7	Ghost 5.35.0 allows authorization bypass: contributors can view draft posts of other users, which is arguably inconsistent with a security policy in which a contributor's draft can only be read by editors until published by an editor. NOTE: the vendor's position is that this behavior has no security impact.	https://ghost.org/docs/security/	A-GHO-GHOS-280323/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26510		
Vendor: Github					
Product: enterprise_server					
Affected Version(s): * Up to (excluding) 3.4.15					
Improper Control of Generation of Code ('Code Injection')	02-Mar-2023	8.8	A code injection vulnerability was identified in GitHub Enterprise Server that allowed setting arbitrary environment variables from a single environment variable value in GitHub Actions when using a Windows based runner. To exploit this vulnerability, an attacker would need existing permission to control the value of environment variables for use with GitHub Actions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.8.0 and was fixed in versions 3.4.15, 3.5.12, 3.6.8, 3.7.5. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-22381**	N/A	A-GIT-ENTE-280323/283
Affected Version(s): * Up to (excluding) 3.4.17					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Mar-2023	8.8	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to versions 3.8 and was fixed in versions 3.7.7, 3.6.10, 3.5.14, and 3.4.17. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23760**	N/A	A-GIT-ENTE-280323/284
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.12					
Improper Control of Generation of Code ('Code Injection')	02-Mar-2023	8.8	A code injection vulnerability was identified in GitHub Enterprise Server that allowed setting arbitrary environment variables from a single environment variable value in GitHub Actions when using a Windows based runner. To	N/A	A-GIT-ENTE-280323/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability, an attacker would need existing permission to control the value of environment variables for use with GitHub Actions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.8.0 and was fixed in versions 3.4.15, 3.5.12, 3.6.8, 3.7.5. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-22381**		
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.14					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Mar-2023	8.8	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to versions 3.8 and was fixed in versions	N/A	A-GIT-ENTE-280323/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.7.7, 3.6.10, 3.5.14, and 3.4.17. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23760**		
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Mar-2023	8.8	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to versions 3.8 and was fixed in versions 3.7.7, 3.6.10, 3.5.14, and 3.4.17. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23760**	N/A	A-GIT-ENTE-280323/287
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.8					
Improper Control of Generation	02-Mar-2023	8.8	A code injection vulnerability was identified in GitHub	N/A	A-GIT-ENTE-280323/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			Enterprise Server that allowed setting arbitrary environment variables from a single environment variable value in GitHub Actions when using a Windows based runner. To exploit this vulnerability, an attacker would need existing permission to control the value of environment variables for use with GitHub Actions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.8.0 and was fixed in versions 3.4.15, 3.5.12, 3.6.8, 3.7.5. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-22381**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.5					
Improper Control of Generation of Code ('Code Injection')	02-Mar-2023	8.8	A code injection vulnerability was identified in GitHub Enterprise Server that allowed setting arbitrary environment variables from a single environment variable value in GitHub Actions when	N/A	A-GIT-ENTE-280323/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a Windows based runner. To exploit this vulnerability, an attacker would need existing permission to control the value of environment variables for use with GitHub Actions. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.8.0 and was fixed in versions 3.4.15, 3.5.12, 3.6.8, 3.7.5. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-22381**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Mar-2023	8.8	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to	N/A	A-GIT-ENTE-280323/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 3.8 and was fixed in versions 3.7.7, 3.6.10, 3.5.14, and 3.4.17. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23760**		
Vendor: github-slug-action_project					
Product: github-slug-action					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.4.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	8.8	github-slug-action is a GitHub Action to expose slug value of GitHub environment variables inside of one's GitHub workflow. Starting in version 4.0.0` and prior to version 4.4.1, this action uses the `github.head_ref` parameter in an insecure way. This vulnerability can be triggered by any user on GitHub on any workflow using the action on pull requests. They just need to create a pull request with a branch name, which can contain the attack payload. This can be used to execute code on the GitHub runners and to exfiltrate any secrets one uses in	https://github.com/rlespinasse/github-slug-action/security/advisories/GHSA-6q4m-7476-932w, https://github.com/rlespinasse/github-slug-action/commit/102b1a064a9b145e56556e22b18b19c624538d94	A-GIT-GITH-280323/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the CI pipeline. A patched action is available in version 4.4.1. No workaround is available. **CVE ID : CVE-2023-27581**		
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 15.7.8					
N/A	09-Mar-2023	2.7	An issue has been discovered in GitLab CE/EE affecting all versions before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A malicious project Maintainer may create a Project Access Token with Owner level privileges using a crafted request. **CVE ID : CVE-2023-1084**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1084.json	A-GIT-GITL-280323/292
Affected Version(s): From (including) 12.1.0 Up to (excluding) 15.7.8					
N/A	09-Mar-2023	3.8	An issue has been discovered in GitLab affecting all versions starting from 12.1 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible for a project	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0483.json	A-GIT-GITL-280323/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maintainer to extract a Datadog integration API key by modifying the site. **CVE ID : CVE-2023-0483**		
Affected Version(s): From (including) 13.7 Up to (excluding) 15.7.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	5.4	An issue has been discovered in GitLab affecting all versions starting from 13.7 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A specially crafted Kroki diagram could lead to a stored XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-0050**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0050.json	A-GIT-GITL-280323/294
Affected Version(s): From (including) 15.5.0 Up to (excluding) 15.7.8					
N/A	09-Mar-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 15.5 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. Non-project members could retrieve release descriptions	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0223.json	A-GIT-GITL-280323/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via the API, even if the release visibility is restricted to project members only in the project settings. **CVE ID : CVE-2023-0223**		
Affected Version(s): From (including) 15.8 Up to (excluding) 15.8.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	5.4	An issue has been discovered in GitLab affecting all versions starting from 13.7 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A specially crafted Kroki diagram could lead to a stored XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims. **CVE ID : CVE-2023-0050**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0050.json	A-GIT-GITL-280323/296
Uncontrolled Resource Consumption	09-Mar-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 9.0 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible to trigger a resource depletion attack due to	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1072.json	A-GIT-GITL-280323/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper filtering for number of requests to read commits details. **CVE ID : CVE-2023-1072**		
Affected Version(s): From (including) 15.8.0 Up to (excluding) 15.8.4					
N/A	09-Mar-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 15.5 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. Non-project members could retrieve release descriptions via the API, even if the release visibility is restricted to project members only in the project settings. **CVE ID : CVE-2023-0223**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0223.json	A-GIT-GITL-280323/298
N/A	09-Mar-2023	3.8	An issue has been discovered in GitLab affecting all versions starting from 12.1 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible for a project maintainer to extract a Datadog integration API key	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0483.json	A-GIT-GITL-280323/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by modifying the site. **CVE ID : CVE-2023-0483**		
N/A	09-Mar-2023	2.7	An issue has been discovered in GitLab CE/EE affecting all versions before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A malicious project Maintainer may create a Project Access Token with Owner level privileges using a crafted request. **CVE ID : CVE-2023-1084**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1084.json	A-GIT-GITL-280323/300
Affected Version(s): From (including) 15.9 Up to (excluding) 15.9.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	5.4	An issue has been discovered in GitLab affecting all versions starting from 13.7 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A specially crafted Kroki diagram could lead to a stored XSS on the client side which allows attackers to perform arbitrary actions on behalf of victims.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0050.json	A-GIT-GITL-280323/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0050		
Uncontrolled Resource Consumption	09-Mar-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 9.0 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible to trigger a resource depletion attack due to improper filtering for number of requests to read commits details. **CVE ID : CVE-2023-1072**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1072.json	A-GIT-GITL-280323/302
Affected Version(s): From (including) 15.9.0 Up to (excluding) 15.9.2					
N/A	09-Mar-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 15.5 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. Non-project members could retrieve release descriptions via the API, even if the release visibility is restricted to project members only in the project settings.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0223.json	A-GIT-GITL-280323/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0223		
N/A	09-Mar-2023	3.8	An issue has been discovered in GitLab affecting all versions starting from 12.1 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible for a project maintainer to extract a Datadog integration API key by modifying the site. **CVE ID : CVE-2023-0483**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0483.json	A-GIT-GITL-280323/304
N/A	09-Mar-2023	2.7	An issue has been discovered in GitLab CE/EE affecting all versions before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. A malicious project Maintainer may create a Project Access Token with Owner level privileges using a crafted request. **CVE ID : CVE-2023-1084**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1084.json	A-GIT-GITL-280323/305
Affected Version(s): From (including) 9.0 Up to (excluding) 15.7.8					
Uncontrolled Resource	09-Mar-2023	5.3	An issue has been discovered in GitLab affecting all versions	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-280323/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			starting from 9.0 before 15.7.8, all versions starting from 15.8 before 15.8.4, all versions starting from 15.9 before 15.9.2. It was possible to trigger a resource depletion attack due to improper filtering for number of requests to read commits details. **CVE ID : CVE-2023-1072**	/blob/master/2023/CVE-2023-1072.json	
Vendor: gitpod					
Product: gitpod					
Affected Version(s): * Up to (excluding) 2022.11.2					
Origin Validation Error	03-Mar-2023	9.6	An issue was discovered in Gitpod versions prior to release-2022.11.2.16. There is a Cross-Site WebSocket Hijacking (CSWSH) vulnerability that allows attackers to make WebSocket connections to the Gitpod JSONRPC server using a victim's credentials, because the Origin header is not restricted. This can lead to the extraction of data from workspaces, to a full takeover of the workspace.	https://app.safebase.io/portal/71ccd717-aa2d-4a1e-942e-c768d37e9e0c/preview?product=default&orgId=71ccd717-aa2d-4a1e-942e-c768d37e9e0c&tcuUid=1d505bda-9a38-4ca5-8724-052e6337f34d, https://github.com/gitpod-	A-GIT-GITP-280323/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0957	io/gitpod/pull/16405	
Vendor: GNU					
Product: emacs					
Affected Version(s): From (including) 28.1 Up to (including) 28.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-Mar-2023	7.8	emacsclient-mail.desktop in Emacs 28.1 through 28.2 is vulnerable to shell command injections through a crafted mailto: URI. This is related to lack of compliance with the Desktop Entry Specification. **CVE ID : CVE-2023-27985**	https://debbugs.gnu.org/cgi/bugreport.cgi?bug=60204, https://www.openwall.com/lists/oss-security/2023/03/08/2, http://git.savannah.gnu.org/cgit/emacs.git/commit/?h=emacs-29&id=d32091199ae5de590a83f1542a01d75fba000467	A-GNU-EMAC-280323/308
Improper Control of Generation of Code ('Code Injection')	09-Mar-2023	7.8	emacsclient-mail.desktop in Emacs 28.1 through 28.2 is vulnerable to Emacs Lisp code injections through a crafted mailto: URI with unescaped double-quote characters. **CVE ID : CVE-2023-27986**	https://www.openwall.com/lists/oss-security/2023/03/08/2, http://git.savannah.gnu.org/cgit/emacs.git/commit/?h=emacs-29&id=3c1693d08b0a71d40a77e7b4	A-GNU-EMAC-280323/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0c0ebc42dca2d2cc, http://www.openwall.com/lists/oss-security/2023/03/09/1	
Product: libredwg					
Affected Version(s): 0.12.5					
Out-of-bounds Write	01-Mar-2023	8.8	A heap-based buffer overflow vulnerability exits in GNU LibreDWG v0.12.5 via the bit_read_RC function at bits.c. **CVE ID : CVE-2023-25222**	https://github.com/LibreDWG/libredwg/issues/615	A-GNU-LIBR-280323/310
Vendor: goauthentik					
Product: authentik					
Affected Version(s): * Up to (excluding) 2022.12.3					
Insufficient Verification of Data Authenticity	04-Mar-2023	6.5	authentik is an open-source Identity Provider. Due to an insufficient access check, a recovery flow link that is created by an admin (or sent via email by an admin) can be used to set the password for any arbitrary user. This attack is only possible if a recovery flow exists, which has both an Identification and an Email stage bound to it. If the flow has policies on the	N/A	A-GOA-AUTH-280323/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identification stage to skip it when the flow is restored (by checking `request.context['is_restored']`), the flow is not affected by this. With this flow in place, an administrator must create a recovery Link or send a recovery URL to the attacker, who can, due to the improper validation of the token create, set the password for any account. Regardless, for custom recovery flows it is recommended to add a policy that checks if the flow is restored, and skips the identification stage. This issue has been fixed in versions 2023.2.3, 2023.1.3 and 2022.12.2. **CVE ID : CVE-2023-26481**		
Affected Version(s): From (excluding) 2023.1.0 Up to (including) 2023.1.3					
Insufficient Verification of Data Authenticity	04-Mar-2023	6.5	authentik is an open-source Identity Provider. Due to an insufficient access check, a recovery flow link that is created by an admin (or sent via email by an admin) can be used to set the	N/A	A-GOA-AUTH-280323/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password for any arbitrary user. This attack is only possible if a recovery flow exists, which has both an Identification and an Email stage bound to it. If the flow has policies on the identification stage to skip it when the flow is restored (by checking `request.context['is_restored']`), the flow is not affected by this. With this flow in place, an administrator must create a recovery Link or send a recovery URL to the attacker, who can, due to the improper validation of the token create, set the password for any account. Regardless, for custom recovery flows it is recommended to add a policy that checks if the flow is restored, and skips the identification stage. This issue has been fixed in versions 2023.2.3, 2023.1.3 and 2022.12.2. **CVE ID : CVE-2023-26481**		
Affected Version(s): From (excluding) 2023.2.0 Up to (including) 2023.2.3					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	04-Mar-2023	6.5	authentik is an open-source Identity Provider. Due to an insufficient access check, a recovery flow link that is created by an admin (or sent via email by an admin) can be used to set the password for any arbitrary user. This attack is only possible if a recovery flow exists, which has both an Identification and an Email stage bound to it. If the flow has policies on the identification stage to skip it when the flow is restored (by checking `request.context['is_restored']`), the flow is not affected by this. With this flow in place, an administrator must create a recovery Link or send a recovery URL to the attacker, who can, due to the improper validation of the token create, set the password for any account. Regardless, for custom recovery flows it is recommended to add a policy that checks if the flow is restored,	N/A	A-GOA-AUTH-280323/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and skips the identification stage. This issue has been fixed in versions 2023.2.3, 2023.1.3 and 2022.12.2. **CVE ID : CVE-2023-26481**		
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.19.7					
Incorrect Calculation	08-Mar-2023	5.3	The ScalarMult and ScalarBaseMult methods of the P256 Curve may return an incorrect result if called with some specific unreduced scalars (a scalar larger than the order of the curve). This does not impact usages of crypto/ecdsa or crypto/ecdh. **CVE ID : CVE-2023-24532**	https://go.dev/cl/471255, https://go.dev/issue/58647	A-GOL-GO-280323/314
Affected Version(s): From (including) 1.20.0 Up to (excluding) 1.20.2					
Incorrect Calculation	08-Mar-2023	5.3	The ScalarMult and ScalarBaseMult methods of the P256 Curve may return an incorrect result if called with some specific unreduced scalars (a scalar larger than the order of the curve). This does not impact usages of	https://go.dev/cl/471255, https://go.dev/issue/58647	A-GOL-GO-280323/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crypto/ecdsa or crypto/ecdh. **CVE ID : CVE-2023-24532**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 111.0.5563.64					
Use After Free	07-Mar-2023	8.8	Use after free in Swiftshader in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1213**	N/A	A-GOO-CHRO-280323/316
Access of Resource Using Incompatible Type ('Type Confusion')	07-Mar-2023	8.8	Type confusion in V8 in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1214**	N/A	A-GOO-CHRO-280323/317
Access of Resource Using Incompatible Type ('Type Confusion')	07-Mar-2023	8.8	Type confusion in CSS in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a	N/A	A-GOO-CHRO-280323/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1215**		
Use After Free	07-Mar-2023	8.8	Use after free in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had convienced the user to engage in direct UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1216**	N/A	A-GOO-CHRO-280323/319
Use After Free	07-Mar-2023	8.8	Use after free in WebRTC in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1218**	N/A	A-GOO-CHRO-280323/320
Out-of-bounds Write	07-Mar-2023	8.8	Heap buffer overflow in Metrics in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to	N/A	A-GOO-CHRO-280323/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1219**		
Out-of-bounds Write	07-Mar-2023	8.8	Heap buffer overflow in UMA in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1220**	N/A	A-GOO-CHRO-280323/322
Out-of-bounds Write	07-Mar-2023	8.8	Heap buffer overflow in Web Audio API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1222**	N/A	A-GOO-CHRO-280323/323
Use After Free	07-Mar-2023	8.8	Use after free in Core in Google Chrome on Lacros prior to 111.0.5563.64 allowed a remote attacker who convinced a user to	N/A	A-GOO-CHRO-280323/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			engage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2023-1227**		
Out-of-bounds Write	07-Mar-2023	6.5	Stack buffer overflow in Crash reporting in Google Chrome on Windows prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1217**	N/A	A-GOO-CHRO-280323/325
N/A	07-Mar-2023	6.5	Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	N/A	A-GOO-CHRO-280323/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1226		
Access of Resource Using Incompatible Type ('Type Confusion')	07-Mar-2023	6.3	Type confusion in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted UI interaction. (Chromium security severity: Low) **CVE ID : CVE-2023-1235**	N/A	A-GOO-CHRO-280323/327
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Extensions API in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium) **CVE ID : CVE-2023-1221**	N/A	A-GOO-CHRO-280323/328
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote	N/A	A-GOO-CHRO-280323/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1223**		
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Web Payments API in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1224**	N/A	A-GOO-CHRO-280323/330
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Navigation in Google Chrome on iOS prior to 111.0.5563.64 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1225**	N/A	A-GOO-CHRO-280323/331
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote	N/A	A-GOO-CHRO-280323/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1228**		
Incorrect Default Permissions	07-Mar-2023	4.3	Inappropriate implementation in Permission prompts in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1229**	N/A	A-GOO-CHRO-280323/333
N/A	07-Mar-2023	4.3	Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious WebApp to spoof the contents of the PWA installer via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1230**	N/A	A-GOO-CHRO-280323/334
N/A	07-Mar-2023	4.3	Inappropriate implementation in	N/A	A-GOO-CHRO-280323/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to potentially spoof the contents of the omnibox via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1231**		
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to obtain potentially sensitive information from API via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1232**	N/A	A-GOO-CHRO-280323/336
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Resource Timing in Google Chrome prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from API via a crafted Chrome Extension.	N/A	A-GOO-CHRO-280323/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Low) **CVE ID : CVE-2023-1233**		
N/A	07-Mar-2023	4.3	Inappropriate implementation in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1234**	N/A	A-GOO-CHRO-280323/338
N/A	07-Mar-2023	4.3	Inappropriate implementation in Internals in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to spoof the origin of an iframe via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1236**	N/A	A-GOO-CHRO-280323/339
Product: youtube_android_player_api					
Affected Version(s): From (including) 1.2 Up to (including) 1.2.2					
Use of Externally-Controlled Input to Select Classes or Code	01-Mar-2023	7.3	The YouTube Embedded 1.2 SDK binds to a service within the YouTube Main App. After binding, a remote context is created	N/A	A-GOO-YOUT-280323/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Unsafe Reflection')			with the flags Context.CONTEXT_INCLUDE_CODE | Context.CONTEXT_IGNORE_SECURITY. This allows the client app to remotely load code from YouTube Main App by retrieving the Main App's ClassLoader. A potential vulnerability in the binding logic used by the client SDK where the SDK ends up calling bindService() on a malicious app rather than YT Main App. This creates a vulnerability where the SDK can load the malicious app's ClassLoader instead, allowing the malicious app to load arbitrary code into the calling app whenever the embedded SDK is invoked. In order to trigger this vulnerability, an attacker must masquerade the Youtube app and install it on a device, have a second app that uses the Embedded player and typically distribute both to the victim outside of the Play Store.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0460		
Vendor: gosaml2_project					
Product: gosaml2					
Affected Version(s): * Up to (excluding) 0.9.0					
N/A	03-Mar-2023	5.3	gosaml2 is a Pure Go implementation of SAML 2.0. SAML Service Providers using this library for SAML authentication support are likely susceptible to Denial of Service attacks. A bug in this library enables attackers to craft a `deflate`-compressed request which will consume significantly more memory during processing than the size of the original request. This may eventually lead to memory exhaustion and the process being killed. The maximum compression ratio achievable with `deflate` is 1032:1, so by limiting the size of bodies passed to gosaml2, limiting the rate and concurrency of calls, and ensuring that lots of memory is available to the process it _may_ be possible to help Go's garbage collector "keep up".	https://github.com/russellhaering/gosaml2/commit/f9d66040241093e8702649baff50cc70d2c683c0, https://github.com/russellhaering/gosaml2/security/advisories/GHSA-6gc3-crp7-25w5	A-GOS-GOSA-280323/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Implementors are encouraged not to rely on this. This issue is fixed in version 0.9.0. **CVE ID : CVE-2023-26483**		
Vendor: goutil_project					
Product: goutil					
Affected Version(s): * Up to (excluding) 0.6.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Mar-2023	8.8	Goutil is a collection of miscellaneous functionality for the go language. In versions prior to 0.6.0 when users use fsutil.Unzip to unzip zip files from a malicious attacker, they may be vulnerable to path traversal. This vulnerability is known as a ZipSlip. This issue has been fixed in version 0.6.0, users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-27475**	https://github.com/gookit/goutil/commit/d7b94fede71f018f129f7d21feb58c895d28dadc, https://github.com/gookit/goutil/security/advisories/GHSA-fx2v-qfhr-4chv	A-GOU-GOUT-280323/342
Vendor: Gradle					
Product: gradle					
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.9.4					
Inclusion of Functionality from Untrusted	02-Mar-2023	9.8	Gradle is a build tool with a focus on build automation and support for multi-language	https://github.com/gradle/gradle/commit/bf3cc0f2b4630330	A-GRA-GRAD-280323/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Control Sphere			development. This is a collision attack on long IDs (64bits) for PGP keys. Users of dependency verification in Gradle are vulnerable if they use long IDs for PGP keys in a `trusted-key` or `pgp` element in their dependency verification metadata file. The fix is to fail dependency verification if anything but a fingerprint is used in a trust element in dependency verification metadata. The problem is fixed in Gradle 8.0 and above. The problem is also patched in Gradle 6.9.4 and 7.6.1. As a workaround, use only full fingerprint IDs for `trusted-key` or `pgp` element in the metadata is a protection against this issue. **CVE ID : CVE-2023-26053**	37e67aaacda31291643ea1a9, https://github.com/gradle/gradle/security/advisories/GHSA-c724-3xg7-g3hf	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.6.1					
Inclusion of Functionality from Untrusted	02-Mar-2023	9.8	Gradle is a build tool with a focus on build automation and support for multi-language development. This is	https://github.com/gradle/gradle/commit/bf3cc0f2b463033037e67aaacda	A-GRA-GRAD-280323/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Control Sphere			a collision attack on long IDs (64bits) for PGP keys. Users of dependency verification in Gradle are vulnerable if they use long IDs for PGP keys in a `trusted-key` or `pgp` element in their dependency verification metadata file. The fix is to fail dependency verification if anything but a fingerprint is used in a trust element in dependency verification metadata. The problem is fixed in Gradle 8.0 and above. The problem is also patched in Gradle 6.9.4 and 7.6.1. As a workaround, use only full fingerprint IDs for `trusted-key` or `pgp` element in the metadata is a protection against this issue. **CVE ID : CVE-2023-26053**	31291643ea1a9, https://github.com/gradle/gradle/security/advisories/GHSA-c724-3xg7-g3hf	
Vendor: grafana					
Product: grafana					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 8.5.21					
Improper Neutralization of Input	01-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability.	https://grafana.com/security/security-	A-GRA-GRAF-280323/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Starting with the 7.0 branch, Grafana had a stored XSS vulnerability in the trace view visualization. The stored XSS vulnerability was possible due the value of a span's attributes/resources were not properly sanitized and this will be rendered when the span's attributes/resources are expanded. An attacker needs to have the Editor role in order to change the value of a trace view visualization to contain JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix. **CVE ID : CVE-2023-0594**	advisories/cve-2023-0594/	
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.5.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. Starting with the 8.1 branch, Grafana had a stored XSS vulnerability affecting the core plugin GeoMap. The stored XSS vulnerability was possible due to map attributions weren't properly sanitized and allowed arbitrary JavaScript to be executed in the context of the currently authorized user of the Grafana instance. An attacker needs to have the Editor role in order to change a panel to include a map attribution containing JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix.	https://grafana.com/security/security-advisories/cve-2023-0507/	A-GRA-GRAF-280323/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0507		
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. On 2023-01-01 during an internal audit of Grafana, a member of the security team found a stored XSS vulnerability affecting the core plugin "Text". The stored XSS vulnerability requires several user interactions in order to be fully exploited. The vulnerability was possible due to React's render cycle that will pass though the unsanitized HTML code, but in the next cycle the HTML is cleaned up and saved in Grafana's database. An attacker needs to have the Editor role in order to change a Text panel to include JavaScript. Another user needs to edit the same Text panel, and click on "Markdown" or "HTML" for the code to be executed. This means that vertical privilege escalation	https://grafana.com/blog/2023/02/28/grafana-security-release-new-versions-with-security-fixes-for-cve-2023-0594-cve-2023-0507-and-cve-2023-22462/, https://github.com/grafana/grafana/commit/db83d5f398caffe35c5846cfa7727d1a2a414165	A-GRA-GRAF-280323/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. This issue has been patched in versions 9.2.10 and 9.3.4. **CVE ID : CVE-2023-22462**		
Affected Version(s): From (including) 9.2.0 Up to (excluding) 9.2.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. Starting with the 8.1 branch, Grafana had a stored XSS vulnerability affecting the core plugin GeoMap. The stored XSS vulnerability was possible due to map attributions weren't properly sanitized and allowed arbitrary JavaScript to be executed in the context of the currently authorized user of the Grafana instance. An attacker needs to have the Editor role in order to change a panel to include a map attribution containing	https://grafana.com/security/security-advisories/cve-2023-0507/	A-GRA-GRAF-280323/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix. **CVE ID : CVE-2023-0507**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. Starting with the 7.0 branch, Grafana had a stored XSS vulnerability in the trace view visualization. The stored XSS vulnerability was possible due the value of a span's attributes/resources were not properly sanitized and this will be rendered when the span's attributes/resources are expanded. An attacker needs to have the Editor role in order to change the value of a trace	https://grafana.com/security/security-advisories/cve-2023-0594/	A-GRA-GRAF-280323/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view visualization to contain JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix. **CVE ID : CVE-2023-0594**		
Affected Version(s): From (including) 9.3.0 Up to (excluding) 9.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. On 2023-01-01 during an internal audit of Grafana, a member of the security team found a stored XSS vulnerability affecting the core plugin "Text". The stored XSS vulnerability requires several user interactions in order to be fully exploited. The vulnerability was possible due to React's render cycle that will pass though the unsanitized	https://grafana.com/blog/2023/02/28/grafana-security-release-new-versions-with-security-fixes-for-cve-2023-0594-cve-2023-0507-and-cve-2023-22462/, https://github.com/grafana/grafana/commit/db83d5f398caffe35c5846cfa7	A-GRA-GRAF-280323/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTML code, but in the next cycle the HTML is cleaned up and saved in Grafana's database. An attacker needs to have the Editor role in order to change a Text panel to include JavaScript. Another user needs to edit the same Text panel, and click on "Markdown" or "HTML" for the code to be executed. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. This issue has been patched in versions 9.2.10 and 9.3.4. **CVE ID : CVE-2023-22462**	727d1a2a414165	
Affected Version(s): From (including) 9.3.0 Up to (excluding) 9.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. Starting with the 8.1 branch, Grafana had a stored XSS vulnerability affecting the core plugin GeoMap. The	https://grafana.com/security/security-advisories/cve-2023-0507/	A-GRA-GRAF-280323/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stored XSS vulnerability was possible due to map attributions weren't properly sanitized and allowed arbitrary JavaScript to be executed in the context of the currently authorized user of the Grafana instance. An attacker needs to have the Editor role in order to change a panel to include a map attribution containing JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix. **CVE ID : CVE-2023-0507**		
Improper Neutralization of Input During Web Page Generation	01-Mar-2023	5.4	Grafana is an open-source platform for monitoring and observability. Starting with the 7.0 branch, Grafana had a stored XSS	https://grafana.com/security/security-advisories/cve-2023-0594/	A-GRA-GRAF-280323/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability in the trace view visualization. The stored XSS vulnerability was possible due the value of a span's attributes/resources were not properly sanitized and this will be rendered when the span's attributes/resources are expanded. An attacker needs to have the Editor role in order to change the value of a trace view visualization to contain JavaScript. This means that vertical privilege escalation is possible, where a user with Editor role can change to a known password for a user having Admin role if the user with Admin role executes malicious JavaScript viewing a dashboard. Users may upgrade to version 8.5.21, 9.2.13 and 9.3.8 to receive a fix. **CVE ID : CVE-2023-0594**		
Vendor: halo					
Product: halo					
Affected Version(s): * Up to (including) 1.6.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	10-Mar-2023	4.8	An arbitrary file upload vulnerability in Halo up to v1.6.1 allows attackers to execute arbitrary code via a crafted .md file. **CVE ID : CVE-2023-27164**	N/A	A-HAL-HALO-280323/353
Vendor: hashicorp					
Product: consul					
Affected Version(s): * Up to (excluding) 1.14.5					
NULL Pointer Dereference	09-Mar-2023	6.5	Consul and Consul Enterprise allowed an authenticated user with service:write permissions to trigger a workflow that causes Consul server and client agents to crash under certain circumstances. This vulnerability was fixed in Consul 1.14.5. **CVE ID : CVE-2023-0845**	https://discuss.hashicorp.com/t/hcsec-2023-06-consul-server-panic-when-ingress-and-api-gateways-configured-with-peering-connections/51197	A-HAS-CONS-280323/354
Product: nomad					
Affected Version(s): 1.5.0					
N/A	14-Mar-2023	8.8	HashiCorp Nomad and Nomad Enterprise 1.5.0 allow a job submitter to escalate to management-level privileges using workload identity and task API. Fixed in 1.5.1.	https://discuss.hashicorp.com/t/hcsec-2023-08-nomad-job-submitter-privilege-escalation-using-workload-	A-HAS-NOMA-280323/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1299	identity/51389	
Missing Authorization	14-Mar-2023	5.3	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.5.0 did not correctly enforce deny policies applied to a workload's variables. Fixed in 1.4.6 and 1.5.1. **CVE ID : CVE-2023-1296**	https://discuss.hashicorp.com/t/hcsec-2023-09-nomad-acls-can-not-deny-access-to-workloads-own-variables/51390	A-HAS-NOMA-280323/356
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.4.6					
Missing Authorization	14-Mar-2023	5.3	HashiCorp Nomad and Nomad Enterprise 1.4.0 up to 1.5.0 did not correctly enforce deny policies applied to a workload's variables. Fixed in 1.4.6 and 1.5.1. **CVE ID : CVE-2023-1296**	https://discuss.hashicorp.com/t/hcsec-2023-09-nomad-acls-can-not-deny-access-to-workloads-own-variables/51390	A-HAS-NOMA-280323/357
Product: vault					
Affected Version(s): * Up to (excluding) 1.10.11					
Incorrect Authorization	11-Mar-2023	8.1	HashiCorp Vault and Vault Enterprise's approle auth method allowed any authenticated user with access to an approle destroy endpoint to destroy the secret ID of any other role by providing the secret ID accessor. This vulnerability is fixed	https://discuss.hashicorp.com/t/hcsec-2023-07-vault-fails-to-verify-if-approle-secretid-belongs-to-role-during-a-destroy-operation/51305	A-HAS-VAUL-280323/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Vault 1.13.0, 1.12.4, 1.11.8, 1.10.11 and above. **CVE ID : CVE-2023-24999**		
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.8					
Incorrect Authorization	11-Mar-2023	8.1	HashiCorp Vault and Vault Enterprise's approle auth method allowed any authenticated user with access to an approle destroy endpoint to destroy the secret ID of any other role by providing the secret ID accessor. This vulnerability is fixed in Vault 1.13.0, 1.12.4, 1.11.8, 1.10.11 and above. **CVE ID : CVE-2023-24999**	https://discuss.hashicorp.com/t/hcsec-2023-07-vault-fails-to-verify-if-approle-secretid-belongs-to-role-during-a-destroy-operation/51305	A-HAS-VAUL-280323/359
Affected Version(s): From (including) 1.12.0 Up to (excluding) 1.12.4					
Incorrect Authorization	11-Mar-2023	8.1	HashiCorp Vault and Vault Enterprise's approle auth method allowed any authenticated user with access to an approle destroy endpoint to destroy the secret ID of any other role by providing the secret ID accessor. This vulnerability is fixed in Vault 1.13.0, 1.12.4, 1.11.8, 1.10.11 and above.	https://discuss.hashicorp.com/t/hcsec-2023-07-vault-fails-to-verify-if-approle-secretid-belongs-to-role-during-a-destroy-operation/51305	A-HAS-VAUL-280323/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24999		
Vendor: hasura					
Product: graphql_engine					
Affected Version(s): * Up to (excluding) 1.3.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	7.5	Hasura is an open-source product that provides users GraphQL or REST APIs. A path traversal vulnerability has been discovered within Hasura GraphQL Engine prior to versions 1.3.4, 2.55.1, 2.20.1, and 2.21.0-beta1. Projects running on Hasura Cloud were not vulnerable. Self-hosted Hasura Projects with deployments that are publicly exposed and not protected by a WAF or other HTTP protection layer should be upgraded to version 1.3.4, 2.55.1, 2.20.1, or 2.21.0-beta1 to receive a patch. **CVE ID : CVE-2023-27588**	https://github.com/hasura/graphql-engine/commit/dda54543ee1ecf647ca5d0971b140c3a7b9f4158, https://github.com/hasura/graphql-engine/security/advisories/GHSA-c9rw-rw2f-mj4x	A-HAS-GRAP-280323/361
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.11.5					
Improper Limitation of a Pathname to a Restricted	14-Mar-2023	7.5	Hasura is an open-source product that provides users GraphQL or REST APIs. A path traversal	https://github.com/hasura/graphql-engine/commit/dda54543ee1ecf647	A-HAS-GRAP-280323/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			vulnerability has been discovered within Hasura GraphQL Engine prior to versions 1.3.4, 2.55.1, 2.20.1, and 2.21.0-beta1. Projects running on Hasura Cloud were not vulnerable. Self-hosted Hasura Projects with deployments that are publicly exposed and not protected by a WAF or other HTTP protection layer should be upgraded to version 1.3.4, 2.55.1, 2.20.1, or 2.21.0-beta1 to receive a patch. **CVE ID : CVE-2023-27588**	ca5d0971b140c3a7b9f4158, https://github.com/hasura/graphql-engine/security/advisories/GHSA-c9rw-rw2f-mj4x	
Affected Version(s): From (including) 2.12.0 Up to (excluding) 2.20.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	7.5	Hasura is an open-source product that provides users GraphQL or REST APIs. A path traversal vulnerability has been discovered within Hasura GraphQL Engine prior to versions 1.3.4, 2.55.1, 2.20.1, and 2.21.0-beta1. Projects running on Hasura Cloud were not vulnerable. Self-hosted Hasura Projects with	https://github.com/hasura/graphql-engine/commit/dda54543ee1ecf647ca5d0971b140c3a7b9f4158, https://github.com/hasura/graphql-engine/security/advisories/GHSA-c9rw-rw2f-mj4x	A-HAS-GRAP-280323/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments that are publicly exposed and not protected by a WAF or other HTTP protection layer should be upgraded to version 1.3.4, 2.55.1, 2.20.1, or 2.21.0-beta1 to receive a patch. **CVE ID : CVE-2023-27588**		
Vendor: health_center_patient_record_management_system_project					
Product: health_center_patient_record_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Health Center Patient Record Management System 1.0. This affects an unknown part of the file login.php. 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-222483. **CVE ID : CVE-2023-1253**	N/A	A-HEA-HEAL-280323/364
Improper Neutralization of	02-Mar-2023	6.1	A vulnerability classified as problematic was	N/A	A-HEA-HEAL-280323/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			found in SourceCodester Health Center Patient Record Management System 1.0. This vulnerability affects unknown code of the file admin/fecalysis_form.php. The manipulation of the argument itr_no leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222220. **CVE ID : CVE-2023-1156**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-2023	6.1	A vulnerability has been found in SourceCodester Health Center Patient Record Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file hematology_print.php. The manipulation of the argument hem_id leads to cross site scripting. The	N/A	A-HEA-HEAL-280323/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222331. **CVE ID : CVE-2023-1180**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	A vulnerability has been found in SourceCodester Health Center Patient Record Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file birthing_print.php. The manipulation of the argument birth_id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222484. **CVE ID : CVE-2023-1254**	N/A	A-HEA-HEAL-280323/367
Vendor: home-assistant					
Product: home-assistant					
Affected Version(s): * Up to (excluding) 2023.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-Mar-2023	10	homeassistant is an open source home automation tool. A remotely exploitable vulnerability bypassing authentication for accessing the Supervisor API through Home Assistant has been discovered. This impacts all Home Assistant installation types that use the Supervisor 2023.01.1 or older. Installation types, like Home Assistant Container (for example Docker), or Home Assistant Core manually in a Python environment, are not affected. The issue has been mitigated and closed in Supervisor version 2023.03.1, which has been rolled out to all affected installations via the auto-update feature of the Supervisor. This rollout has been completed at the time of publication of this advisory. Home Assistant Core 2023.3.0 included mitigation for this vulnerability. Upgrading to at least that version is thus	https://github.com/home-assistant/core/security/advisories/GHSA-2j8f-h4mr-qr25, https://www.home-assistant.io/blog/2023/03/08/supervisor-security-disclosure/	A-HOM-HOME-280323/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			advised. In case one is not able to upgrade the Home Assistant Supervisor or the Home Assistant Core application at this time, it is advised to not expose your Home Assistant instance to the internet. **CVE ID : CVE-2023-27482**		
Product: supervisor					
Affected Version(s): * Up to (excluding) 2023.03.1					
Improper Authentication	08-Mar-2023	10	homeassistant is an open source home automation tool. A remotely exploitable vulnerability bypassing authentication for accessing the Supervisor API through Home Assistant has been discovered. This impacts all Home Assistant installation types that use the Supervisor 2023.01.1 or older. Installation types, like Home Assistant Container (for example Docker), or Home Assistant Core manually in a Python environment, are not affected. The issue has been mitigated and closed in	https://github.com/home-assistant/core/security/advisories/GHSA-2j8f-h4mr-qr25, https://www.home-assistant.io/blog/2023/03/08/supervisor-security-disclosure/	A-HOM-SUPE-280323/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supervisor version 2023.03.1, which has been rolled out to all affected installations via the auto-update feature of the Supervisor. This rollout has been completed at the time of publication of this advisory. Home Assistant Core 2023.3.0 included mitigation for this vulnerability. Upgrading to at least that version is thus advised. In case one is not able to upgrade the Home Assistant Supervisor or the Home Assistant Core application at this time, it is advised to not expose your Home Assistant instance to the internet. **CVE ID : CVE-2023-27482**		
Vendor: hornerautomation					
Product: cscape_envision_rv					
Affected Version(s): 4.60					
Out-of-bounds Read	09-Mar-2023	7.8	Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds read vulnerability when parsing project (i.e. HMI) files. The product lacks proper	N/A	A-HOR-CSCA-280323/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data, which could result in reads past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-0621**		
Out-of-bounds Write	09-Mar-2023	7.8	Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds write vulnerability when parsing project (i.e. HMI) files. The product lacks proper validation of user-supplied data, which could result in writes past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-0622**	N/A	A-HOR-CSCA-280323/371
Out-of-bounds Write	09-Mar-2023	7.8	Cscape Envision RV version 4.60 is vulnerable to an out-of-bounds write vulnerability when parsing project (i.e. HMI) files. The	N/A	A-HOR-CSCA-280323/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product lacks proper validation of user-supplied data, which could result in writes past the end of allocated data structures. An attacker could leverage these vulnerabilities to execute arbitrary code in the context of the current process. **CVE ID : CVE-2023-0623**		
Vendor: hsycms					
Product: hsycms					
Affected Version(s): 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in Hsycms 3.1. Affected by this issue is some unknown functionality of the file controller\cate.php of the component Add Category Module. The manipulation of the argument title leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222842 is the	N/A	A-HSY-HSYC-280323/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. **CVE ID : CVE-2023-1349**		
Vendor: i2_pros_\&_cons_project					
Product: i2_pros_\&_cons					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The i2 Pros & Cons WordPress plugin through 1.3.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0065**	N/A	A-I2_-I2_P-280323/374
Vendor: IBM					
Product: http_server					
Affected Version(s): 8.5.0.0					
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	https://www.ibm.com/support/pages/node/6958522, https://exchange.xforce.ibmcloud.com/vulnerabilities/248296	A-IBM-HTTP-280323/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mq_certified_container					
Affected Version(s): From (including) 9.3.0.1 Up to (excluding) 9.3.0.4					
N/A	15-Mar-2023	8.8	IBM MQ Certified Container 9.3.0.1 through 9.3.0.3 and 9.3.1.0 through 9.3.1.1 could allow authenticated users with the cluster to be granted administration access to the MQ console due to improper access controls. IBM X-Force ID: 248417. **CVE ID : CVE-2023-26284**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248417, https://www.ibm.com/support/pages/node/6960201	A-IBM-MQ_C-280323/376
Affected Version(s): From (including) 9.3.1.0 Up to (excluding) 9.3.2.0					
N/A	15-Mar-2023	8.8	IBM MQ Certified Container 9.3.0.1 through 9.3.0.3 and 9.3.1.0 through 9.3.1.1 could allow authenticated users with the cluster to be granted administration access to the MQ console due to improper access controls. IBM X-Force ID: 248417. **CVE ID : CVE-2023-26284**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248417, https://www.ibm.com/support/pages/node/6960201	A-IBM-MQ_C-280323/377
Product: observability_with_instana					
Affected Version(s): 243-0					
Missing Authentication for	03-Mar-2023	9.1	Docker based datastores for IBM Instana (IBM Observability with	https://www.ibm.com/support/pages/node/695	A-IBM-OBSE-280323/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			Instana 239-0 through 239-2, 241-0 through 241-2, and 243-0) do not currently require authentication. Due to this, an attacker within the network could access the datastores with read/write access. IBM X-Force ID: 248737. **CVE ID : CVE-2023-27290**	9969, https://exchange.xforce.ibmcloud.com/vulnerabilities/248737	
Affected Version(s): From (including) 239-0 Up to (including) 239-2					
Missing Authentication for Critical Function	03-Mar-2023	9.1	Docker based datastores for IBM Instana (IBM Observability with Instana 239-0 through 239-2, 241-0 through 241-2, and 243-0) do not currently require authentication. Due to this, an attacker within the network could access the datastores with read/write access. IBM X-Force ID: 248737. **CVE ID : CVE-2023-27290**	https://www.ibm.com/support/pages/node/6959969, https://exchange.xforce.ibmcloud.com/vulnerabilities/248737	A-IBM-OBSE-280323/379
Affected Version(s): From (including) 241-0 Up to (including) 241-2					
Missing Authentication for Critical Function	03-Mar-2023	9.1	Docker based datastores for IBM Instana (IBM Observability with Instana 239-0 through 239-2, 241-	https://www.ibm.com/support/pages/node/6959969, https://exch	A-IBM-OBSE-280323/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0 through 241-2, and 243-0) do not currently require authentication. Due to this, an attacker within the network could access the datastores with read/write access. IBM X-Force ID: 248737. **CVE ID : CVE-2023-27290**	ange.xforce.ibmcloud.com/vulnerabilities/248737	
Product: robotic_process_automation					
Affected Version(s): * Up to (excluding) 21.0.6					
N/A	15-Mar-2023	6.5	IBM Robotic Process Automation 21.0.1 through 21.0.5 is vulnerable to insufficiently protecting credentials. Queue Provider credentials are not obfuscated while editing queue provider details. IBM X-Force ID: 247032. **CVE ID : CVE-2023-25680**	https://www.ibm.com/support/pages/node/6962207, https://exchange.xforce.ibmcloud.com/vulnerabilities/247032	A-IBM-ROBO-280323/381
Affected Version(s): From (including) 21.0.1 Up to (excluding) 21.0.7.1					
Insufficient Session Expiration	15-Mar-2023	3.2	IBM Robotic Process Automation 21.0.1 through 21.0.7 and 23.0.0 through 23.0.1 could allow a user with physical access to the system due to session tokens for not being invalidated after a password	https://www.ibm.com/support/pages/node/6962175, https://exchange.xforce.ibmcloud.com/vulnerabilities/243710	A-IBM-ROBO-280323/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset. IBM X-Force ID: 243710. **CVE ID : CVE-2023-22591**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.2					
Insufficient Session Expiration	15-Mar-2023	3.2	IBM Robotic Process Automation 21.0.1 through 21.0.7 and 23.0.0 through 23.0.1 could allow a user with physical access to the system due to session tokens for not being invalidated after a password reset. IBM X-Force ID: 243710. **CVE ID : CVE-2023-22591**	https://www.ibm.com/support/pages/node/6962175, https://exchange.xforce.ibmcloud.com/vulnerabilities/243710	A-IBM-ROBO-280323/383
Product: robotic_process_automation_as_a_service					
Affected Version(s): * Up to (excluding) 21.0.6					
N/A	15-Mar-2023	6.5	IBM Robotic Process Automation 21.0.1 through 21.0.5 is vulnerable to insufficiently protecting credentials. Queue Provider credentials are not obfuscated while editing queue provider details. IBM X-Force ID: 247032. **CVE ID : CVE-2023-25680**	https://www.ibm.com/support/pages/node/6962207, https://exchange.xforce.ibmcloud.com/vulnerabilities/247032	A-IBM-ROBO-280323/384
Affected Version(s): * Up to (excluding) 23.0.2					
Insufficient Session Expiration	15-Mar-2023	3.2	IBM Robotic Process Automation 21.0.1 through 21.0.7 and 23.0.0 through 23.0.1 could allow a user	https://www.ibm.com/support/pages/node/6962175,	A-IBM-ROBO-280323/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system due to session tokens for not being invalidated after a password reset. IBM X-Force ID: 243710. **CVE ID : CVE-2023-22591**	https://exchange.xforce.ibmcloud.com/vulnerabilities/243710	
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): From (including) 21.0.1 Up to (excluding) 21.0.6					
N/A	15-Mar-2023	6.5	IBM Robotic Process Automation 21.0.1 through 21.0.5 is vulnerable to insufficiently protecting credentials. Queue Provider credentials are not obfuscated while editing queue provider details. IBM X-Force ID: 247032. **CVE ID : CVE-2023-25680**	https://www.ibm.com/support/pages/node/6962207, https://exchange.xforce.ibmcloud.com/vulnerabilities/247032	A-IBM-ROBO-280323/386
Product: spectrum_symphony					
Affected Version(s): 7.3.0					
Improper Input Validation	10-Mar-2023	6.1	IBM Spectrum Symphony 7.3 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache	https://exchange.xforce.ibmcloud.com/vulnerabilities/247030, https://www.ibm.com/support/pages/node/6959369	A-IBM-SPEC-280323/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			poisoning or session hijacking. IBM X-Force ID: 247030. **CVE ID : CVE-2023-24975**		
Product: sterling_b2b_integrator					
Affected Version(s): From (including) 6.0.0.0 Up to (excluding) 6.0.3.8					
N/A	15-Mar-2023	6.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.7 and 6.1.0.0 through 6.1.2.1 could allow a privileged user to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 244364. **CVE ID : CVE-2023-22876**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244364, https://www.ibm.com/support/pages/node/6963093	A-IBM-STER-280323/388
Affected Version(s): From (including) 6.1.0.0 Up to (excluding) 6.1.2.2					
N/A	15-Mar-2023	6.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.7 and 6.1.0.0 through 6.1.2.1 could allow a privileged user to obtain sensitive information that could aid in further attacks against the system. IBM X-Force ID: 244364. **CVE ID : CVE-2023-22876**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244364, https://www.ibm.com/support/pages/node/6963093	A-IBM-STER-280323/389
Vendor: ibos					
Product: ibos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	6.1	A vulnerability, which was classified as problematic, has been found in IBOS up to 4.5.5. Affected by this issue is some unknown functionality of the file mobil/index.php. The manipulation of the argument accesstoken leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-222608. **CVE ID : CVE-2023-1278**	https://gitee.com/ibos/IBOS/issues/I6G5IJ	A-IBO-IBOS-280323/390
Vendor: imageinfo_project					
Product: imageinfo					
Affected Version(s): * Up to (including) 3.0.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Mar-2023	7.8	A vulnerability was found in xiaozhuai imageinfo up to 3.0.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file imageinfo.hpp. The manipulation leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. VDB-222362 is	N/A	A-IMA-IMAG-280323/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1190**		
Vendor: inscada_project					
Product: inscada					
Affected Version(s): * Up to (excluding) 20230115-1					
N/A	06-Mar-2023	9.8	Improper Protection for Outbound Error Messages and Alert Signals vulnerability in ProMIS Process Co. InSCADA allows Account Footprinting.This issue affects inSCADA: before 20230115-1. **CVE ID : CVE-2023-0839**	N/A	A-INS-INSC-280323/392
Vendor: jeecg					
Product: jeecg					
Affected Version(s): 3.4.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Mar-2023	8.8	jeecg-boot v3.4.4 was discovered to contain an authenticated SQL injection vulnerability via the building block report component. **CVE ID : CVE-2023-24789**	N/A	A-JEE-JEEC-280323/393
Vendor: jellyfin					
Product: jellyfin					
Affected Version(s): * Up to (including) 10.7.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	10-Mar-2023	7.5	Jellyfin up to v10.7.7 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /Repositories. This vulnerability allows attackers to access network resources and sensitive information via a crafted POST request. **CVE ID : CVE-2023-27161**	N/A	A-JEL-JELL-280323/394
Vendor: Jenkins					
Product: jenkins					
Affected Version(s): * Up to (excluding) 2.375.4					
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier uses the Apache Commons FileUpload library without specifying limits for the number of request parts introduced in version 1.5 for CVE-2023-24998 in hudson.util.MultipartFormDataParser, allowing attackers to trigger a denial of service. **CVE ID : CVE-2023-27900**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3030	A-JEN-JENK-280323/395
Allocation of Resources Without	10-Mar-2023	7.5	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier uses the Apache Commons FileUpload library	https://www.jenkins.io/security/advisory/2023-03-	A-JEN-JENK-280323/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			without specifying limits for the number of request parts introduced in version 1.5 for CVE-2023-24998 in org.kohsuke.stapler.RequestImpl, allowing attackers to trigger a denial of service. **CVE ID : CVE-2023-27901**	08/#SECURITY-3030	
Incorrect Authorization	10-Mar-2023	7	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier creates a temporary file in the default temporary directory with the default permissions for newly created files when uploading a plugin for installation, potentially allowing attackers with access to the Jenkins controller file system to read and write the file before it is used, potentially resulting in arbitrary code execution. **CVE ID : CVE-2023-27899**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-2823	A-JEN-JENK-280323/397
N/A	10-Mar-2023	5.3	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier prints an error stack trace on agent-related pages when agent connections are broken, potentially	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-2120	A-JEN-JENK-280323/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			revealing information about Jenkins configuration that is otherwise inaccessible to attackers. **CVE ID : CVE-2023-27904**		
Incorrect Authorization	10-Mar-2023	4.4	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier creates a temporary file in the default temporary directory with the default permissions for newly created files when uploading a file parameter through the CLI, potentially allowing attackers with access to the Jenkins controller file system to read and write the file before it is used. **CVE ID : CVE-2023-27903**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3058	A-JEN-JENK-280323/399
N/A	10-Mar-2023	4.3	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier shows temporary directories related to job workspaces, which allows attackers with Item/Workspace permission to access their contents. **CVE ID : CVE-2023-27902**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-1807	A-JEN-JENK-280323/400
Affected Version(s): * Up to (excluding) 2.394					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier uses the Apache Commons FileUpload library without specifying limits for the number of request parts introduced in version 1.5 for CVE-2023-24998 in hudson.util.MultipartFormDataParser, allowing attackers to trigger a denial of service. **CVE ID : CVE-2023-27900**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3030	A-JEN-JENK-280323/401
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier uses the Apache Commons FileUpload library without specifying limits for the number of request parts introduced in version 1.5 for CVE-2023-24998 in org.kohsuke.stapler.RequestImpl, allowing attackers to trigger a denial of service. **CVE ID : CVE-2023-27901**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3030	A-JEN-JENK-280323/402
Incorrect Authorization	10-Mar-2023	7	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier creates a temporary file in the default temporary directory with the default permissions	https://www.jenkins.io/security/advisory/2023-03-	A-JEN-JENK-280323/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for newly created files when uploading a plugin for installation, potentially allowing attackers with access to the Jenkins controller file system to read and write the file before it is used, potentially resulting in arbitrary code execution. **CVE ID : CVE-2023-27899**	08/#SECURITY-2823	
N/A	10-Mar-2023	5.3	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier prints an error stack trace on agent-related pages when agent connections are broken, potentially revealing information about Jenkins configuration that is otherwise inaccessible to attackers. **CVE ID : CVE-2023-27904**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-2120	A-JEN-JENK-280323/404
Incorrect Authorization	10-Mar-2023	4.4	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier creates a temporary file in the default temporary directory with the default permissions for newly created files when uploading a file parameter through the CLI, potentially allowing	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3058	A-JEN-JENK-280323/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with access to the Jenkins controller file system to read and write the file before it is used. **CVE ID : CVE-2023-27903**		
N/A	10-Mar-2023	4.3	Jenkins 2.393 and earlier, LTS 2.375.3 and earlier shows temporary directories related to job workspaces, which allows attackers with Item/Workspace permission to access their contents. **CVE ID : CVE-2023-27902**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-1807	A-JEN-JENK-280323/406
Affected Version(s): From (including) 2.270 Up to (excluding) 2.394					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Jenkins 2.270 through 2.393 (both inclusive), LTS 2.277.1 through 2.375.3 (both inclusive) does not escape the Jenkins version a plugin depends on when rendering the error message stating its incompatibility with the current version of Jenkins, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide plugins to the configured	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3037	A-JEN-JENK-280323/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			update sites and have this message shown by Jenkins instances. **CVE ID : CVE-2023-27898**		
Affected Version(s): From (including) 2.277.1 Up to (excluding) 2.375.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Jenkins 2.270 through 2.393 (both inclusive), LTS 2.277.1 through 2.375.3 (both inclusive) does not escape the Jenkins version a plugin depends on when rendering the error message stating its incompatibility with the current version of Jenkins, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide plugins to the configured update sites and have this message shown by Jenkins instances. **CVE ID : CVE-2023-27898**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3037	A-JEN-JENK-280323/408
Product: update-center2					
Affected Version(s): 3.13					
Improper Neutralization of Input During Web Page	10-Mar-2023	5.4	Jenkins update-center2 3.13 and 3.14 renders the required Jenkins core version on plugin download	https://www.jenkins.io/security/advisory/2023-03-	A-JEN-UPDA-280323/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			index pages without sanitization, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a plugin for hosting. **CVE ID : CVE-2023-27905**	08/#SECURITY-3063	
Affected Version(s): 3.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	5.4	Jenkins update-center2 3.13 and 3.14 renders the required Jenkins core version on plugin download index pages without sanitization, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a plugin for hosting. **CVE ID : CVE-2023-27905**	https://www.jenkins.io/security/advisory/2023-03-08/#SECURITY-3063	A-JEN-UPDA-280323/410
Vendor: jizhicms					
Product: jizhicms					
Affected Version(s): 2.4.5					
Unrestricted Upload of File with Dangerous Type	15-Mar-2023	7.2	An arbitrary file upload vulnerability in the \admin\c\CommonController.php component of Jizhicms v2.4.5 allows attackers to execute arbitrary	N/A	A-JIZ-JIZH-280323/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via a crafted phtml file. **CVE ID : CVE-2023-27235**		
Cross-Site Request Forgery (CSRF)	15-Mar-2023	6.5	A Cross-Site Request Forgery (CSRF) in /Sys/index.html of Jizhicms v2.4.5 allows attackers to arbitrarily make configuration changes within the application. **CVE ID : CVE-2023-27234**	N/A	A-JIZ-JIZH-280323/412
Vendor: jpegoptim_project					
Product: jpegoptim					
Affected Version(s): 1.5.2					
Out-of-bounds Write	15-Mar-2023	7.8	jpegoptim v1.5.2 was discovered to contain a heap overflow in the optimize function at jpegoptim.c. **CVE ID : CVE-2023-27781**	https://github.com/tjko/jpegoptim/issues/132	A-JPE-JPEG-280323/413
Vendor: jtekt					
Product: kostac_plc_programming_software					
Affected Version(s): * Up to (including) 1.6.9.0					
Out-of-bounds Read	06-Mar-2023	7.8	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.9.0 and earlier. When processing a comment block in	https://www.electronics.jtekt.co.jp/jp/topics/202303031363 9/, https://www.electronics.jtekt.co.jp/en/topics/20	A-JTE-KOST-280323/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stage information, the end of data cannot be verified and out-of-bounds read occurs. As a result, opening a specially crafted project file may lead to information disclosure and/or arbitrary code execution. **CVE ID : CVE-2023-22419**	2303035258/	
Out-of-bounds Read	06-Mar-2023	7.8	Out-of-bounds read vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC Programming Software) Version 1.6.9.0 and earlier. The insufficient buffer size for the PLC program instructions leads to out-of-bounds read. As a result, opening a specially crafted project file may lead to information disclosure and/or arbitrary code execution. **CVE ID : CVE-2023-22421**	https://www.electronics.jtekt.co.jp/jp/topics/202303031363 9/, https://www.electronics.jtekt.co.jp/en/topics/202303035258/	A-JTE-KOST-280323/415
Use After Free	06-Mar-2023	7.8	Use-after-free vulnerability exists in Kostac PLC Programming Software (Former name: Koyo PLC	https://www.electronics.jtekt.co.jp/jp/topics/202303031363 9/,	A-JTE-KOST-280323/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Programming Software) Version 1.6.9.0 and earlier. With the abnormal value given as the maximum number of columns for the PLC program, the process accesses the freed memory. As a result, opening a specially crafted project file may lead to information disclosure and/or arbitrary code execution. **CVE ID : CVE-2023-22424**	https://www.electronics.jtekt.co.jp/en/topics/202303035258/	
Vendor: judging_management_system_project					
Product: judging_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the sid parameter at /php-jms/updateview.php. **CVE ID : CVE-2023-24641**	N/A	A-JUD-JUDG-280323/417
Improper Neutralization of Special Elements used in an SQL Command	03-Mar-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the sid parameter at /php-	N/A	A-JUD-JUDG-280323/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			jms/updateTxtview.php. **CVE ID : CVE-2023-24642**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the sid parameter at /php-jms/updateBlankTxtview.php. **CVE ID : CVE-2023-24643**	N/A	A-JUD-JUDG-280323/419
Vendor: kdab					
Product: hotspot					
Affected Version(s): From (including) 1.3.0 Up to (including) 1.4.1					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	KDAB Hotspot 1.3.x and 1.4.x through 1.4.1, in a non-default configuration, allows privilege escalation because of race conditions involving symlinks and elevate_perf_privileges.sh chown calls. **CVE ID : CVE-2023-28144**	N/A	A-KDA-HOTS-280323/420
Vendor: Kibokolabs					
Product: namaste\!_lms					
Affected Version(s): * Up to (excluding) 2.6					
Improper Neutralization of Input During	13-Mar-2023	4.8	The Namaste! LMS WordPress plugin before 2.6 does not sanitize and escape some of its settings,	N/A	A-KIB-NAMA-280323/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			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-2023-0844**		
Product: watu_quiz					
Affected Version(s): * Up to (including) 3.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	The Watu Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dn', 'email', 'points', and 'date' parameters in versions up to, and including, 3.3.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-0968**	N/A	A-KIB-WATU-280323/422
Vendor: kitabisa					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: teler-waf					
Affected Version(s): * Up to (excluding) 0.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	6.1	teler-waf is a Go HTTP middleware that provides teler IDS functionality to protect against web-based attacks. In teler-waf prior to version 0.1.1 is vulnerable to bypassing common web attack rules when a specific HTML entities payload is used. This vulnerability allows an attacker to execute arbitrary JavaScript code on the victim's browser and compromise the security of the web application. The vulnerability exists due to teler-waf failure to properly sanitize and filter HTML entities in user input. An attacker can exploit this vulnerability to bypass common web attack threat rules in teler-waf and launch cross-site scripting (XSS) attacks. The attacker can execute arbitrary JavaScript code on the victim's browser and steal sensitive information, such as	https://github.com/kitabisa/teler-waf/commit/d1d49cfddfa3ec2adad962870f14b85cd1aaf739, https://github.com/kitabisa/teler-waf/security/advisories/GHSA-9f95-hhg4-pg4f	A-KIT-TELE-280323/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			login credentials and session tokens, or take control of the victim's browser and perform malicious actions. This issue has been fixed in version 0.1.1. **CVE ID : CVE-2023-26046**		
Affected Version(s): * Up to (excluding) 0.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	teler-waf is a Go HTTP middleware that provides teler IDS functionality to protect against web-based attacks. In teler-waf prior to version v0.2.0 is vulnerable to a bypass attack when a specific case-sensitive hex entities payload with special characters such as CR/LF and horizontal tab is used. This vulnerability allows an attacker to execute arbitrary JavaScript code on the victim's browser and compromise the security of the web application. An attacker can exploit this vulnerability to bypass common web attack threat rules in teler-waf and launch cross-site scripting (XSS) attacks. The	https://github.com/dwisiswant0/cwa-filter-rules/commit/d818d1645832d1a02cd210c7680e692d2bf4313b	A-KIT-TELE-280323/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can execute arbitrary JavaScript code on the victim's browser and steal sensitive information, such as login credentials and session tokens, or take control of the victim's browser and perform malicious actions. This issue has been patched in version 0.2.0. **CVE ID : CVE-2023-26047**		
Vendor: libelfin_project					
Product: libelfin					
Affected Version(s): 0.3					
Integer Overflow or Wraparound	14-Mar-2023	6.5	Libelfin v0.3 was discovered to contain an integer overflow in the load function at elf/mmap_loader.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted elf file. **CVE ID : CVE-2023-24180**	N/A	A-LIB-LIBE-280323/425
Vendor: libmemcached-awesome_project					
Product: libmemcached-awesome					
Affected Version(s): From (including) 1.0.18 Up to (excluding) 1.1.4					
Exposure of Sensitive Information to an	07-Mar-2023	6.5	libmemcached-awesome is an open source C/C++ client library and tools for the memcached server.	https://github.com/awesomized/libmemcached/security/advisories/GHSA	A-LIB-LIBM-280323/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			`libmemcached` could return data for a previously requested key, if that previous request timed out due to a low `POLL_TIMEOUT`. This issue has been addressed in version 1.1.4. Users are advised to upgrade. There are several ways to workaround or lower the probability of this bug affecting a given deployment. 1: use a reasonably high `POLL_TIMEOUT` setting, like the default. 2: use separate libmemcached connections for unrelated data. 3: do not re-use libmemcached connections in an unknown state. **CVE ID : CVE-2023-27478**	-wwmh-39wj-fx59, https://github.com/awesomized/libmemcached/commit/48dcc61a, https://github.com/php-memcached-dev/php-memcached/issues/531	
Vendor: liferea_project					
Product: liferea					
Affected Version(s): * Up to (excluding) 1.14.1					
Improper Neutralization of Special Elements used in an OS	11-Mar-2023	9.8	A vulnerability was found in liferea. It has been rated as critical. Affected by this issue is the function update_job_run of	https://github.com/lwindolf/liferea/commit/8d8b5b963fa64c7a2122d1bbf	A-LIF-LIFE-280323/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			the file src/update.c of the component Feed Enrichment. The manipulation of the argument source with the input |date >/tmp/bad-item-link.txt leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 8d8b5b963fa64c7a2122d1bbfbb0bed46e813e59. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-222848. **CVE ID : CVE-2023-1350**	bb0bed46e813e59	
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Out-of-bounds Read	10-Mar-2023	4.4	NVIDIA CUDA Toolkit SDK contains a vulnerability in cuobjdump, where a local user running the tool against a malicious binary may cause an out-of-bounds read, which may result in a limited denial of service and limited	https://nvidia.custhelp.com/app/answers/detail/a_id/5446	A-LIN-LINU-280323/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2023-0193**		
NULL Pointer Dereference	02-Mar-2023	3.3	NVIDIA CUDA Toolkit SDK contains a bug in cuobjdump, where a local user running the tool against an ill-formed binary may cause a null- pointer dereference, which may result in a limited denial of service. **CVE ID : CVE-2023-0196**	https://nvidia.custhelp.com/app/answers/detail/a_id/5446	A-LIN-LINU-280323/429
Vendor: Linuxfoundation					
Product: runc					
Affected Version(s): * Up to (including) 1.1.4					
Use of Incorrectly-Resolved Name or Reference	03-Mar-2023	7	runc through 1.1.4 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. NOTE: this issue exists because of a CVE-2019-19921 regression.	N/A	A-LIN-RUNC-280323/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27561		
Vendor: live2d					
Product: cubism_editor					
Affected Version(s): 4.2.03					
Out-of-bounds Write	03-Mar-2023	7.8	Cubism Core in Live2D Cubism Editor 4.2.03 allows out-of-bounds write via a crafted Section Offset Table or Count Info Table in an MOC3 file. **CVE ID : CVE-2023-27566**	N/A	A-LIV-CUBI-280323/431
Vendor: lmxcms					
Product: lmxcms					
Affected Version(s): 1.41					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	A vulnerability has been found in lmxcms 1.41 and classified as critical. Affected by this vulnerability is the function update of the file AcquisiAction.class.php. The manipulation of the argument id with the input -1 and updatexml(0,concat(0x7e,user()),1)# leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-LMX-LMXC-280323/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-222727. **CVE ID : CVE-2023-1321**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	A vulnerability was found in lmxcms 1.41 and classified as critical. Affected by this issue is the function reply of the file BookAction.class.php. The manipulation of the argument id with the input 1) and updatexml(0,concat(0x7e,user()),1)# leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222728. **CVE ID : CVE-2023-1322**	N/A	A-LMX-LMXC-280323/433
Vendor: loonflow_project					
Product: loonflow					
Affected Version(s): r2.0.14					
Server-Side Request Forgery (SSRF)	07-Mar-2023	4.9	loonflow r2.0.14 is vulnerable to server-side request forgery (SSRF). **CVE ID : CVE-2023-25230**	N/A	A-LOO-LOON-280323/434
Vendor: Lsoft					
Product: listserv					
Affected Version(s): * Up to (excluding) 17.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Mar-2023	6.1	The REPORT (after z but before a) parameter in wa.exe in L-Soft LISTSERV 16.5 before 17 allows an attacker to conduct XSS attacks via a crafted URL. **CVE ID : CVE-2023-27641**	N/A	A-LSO-LIST-280323/435
Vendor: maddy_project					
Product: maddy					
Affected Version(s): From (including) 0.2.0 Up to (excluding) 0.6.3					
Improper Authentication	13-Mar-2023	9.8	maddy is a composable, all-in-one mail server. Starting with version 0.2.0 and prior to version 0.6.3, maddy allows a full authentication bypass if SASL authorization username is specified when using the PLAIN authentication mechanisms. Instead of validating the specified username, it is accepted as is after checking the credentials for the authentication username. maddy 0.6.3 includes the fix for the bug. There are no known workarounds. **CVE ID : CVE-2023-27582**	https://github.com/foxcpp/maddy/security/advisories/GHSA-4g76-w3xw-2x6w, https://github.com/foxcpp/maddy/commit/55a91a37b71210f34f98f4d327c30308fe24399a, https://github.com/foxcpp/maddy/commit/9f58cb64b39cdc01928ec463bdb198c4c2313a9c	A-MAD-MADD-280323/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Mailcow					
Product: mailcow					
Affected Version(s): _dockerized Up to (excluding) 2023-03					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Mar-2023	8.8	mailcow is a dockerized email package, with multiple containers linked in one bridged network. The Sync Job feature - which can be made available to standard users by assigning them the necessary permission - suffers from a shell command injection. A malicious user can abuse this vulnerability to obtain shell access to the Docker container running dovecot. The imapsync Perl script implements all the necessary functionality for this feature, including the XOAUTH2 authentication mechanism. This code path creates a shell command to call openssl. However, since different parts of the specified user password are included without any validation, one can simply execute additional shell commands. Notably,	N/A	A-MAI-MAIL-280323/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the default ACL for a newly-created mailcow account does not include the necessary permission. The Issue has been fixed within the 2023-03 Update (March 3rd 2023). As a temporary workaround the Syncjob ACL can be removed from all mailbox users, preventing from creating or changing existing Syncjobs. **CVE ID : CVE-2023-26490**		
Vendor: mattermost					
Product: mattermost_server					
Affected Version(s): From (including) 5.32.0 Up to (excluding) 7.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Mar-2023	6.1	A reflected cross-site scripting vulnerability in the OAuth flow completion endpoints in Mattermost allows an attacker to send AJAX requests on behalf of the victim via sharing a crafted link with a malicious state parameter. **CVE ID : CVE-2023-1421**	https://mattermost.com/security-updates/	A-MAT-MATT-280323/438
Vendor: Mcafee					
Product: advanced_threat_defense					
Affected Version(s): From (including) 4.0 Up to (including) 4.14.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	6.7	A command injection vulnerability in Trellix Intelligent Sandbox CLI for version 5.2 and earlier, allows a local user to inject and execute arbitrary operating system commands using specially crafted strings. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI command. The vulnerability allows the attack **CVE ID : CVE-2023-0978**	https://kcm.trellix.com/corporate/index?page=content&id=SB10397	A-MCA-ADVA-280323/439
Product: total_protection					
Affected Version(s): * Up to (excluding) 16.0.49					
Uncontrolled Search Path Element	13-Mar-2023	5.5	McAfee Total Protection prior to 16.0.49 allows attackers to elevate user privileges due to DLL sideloading. This could enable a user with lower privileges to execute unauthorized tasks. **CVE ID : CVE-2023-24578**	https://www.mcafee.com/en-us/consumer-corporate/mcafee-labs/product-security-bulletins.html, https://www.mcafee.com/support/?articleId=TS103397&page=shell&shel	A-MCA-TOTA-280323/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				l=article-view	
Affected Version(s): * Up to (excluding) 16.0.50					
Improper Link Resolution Before File Access ('Link Following')	13-Mar-2023	5.5	McAfee Total Protection prior to 16.0.50 allows attackers to elevate user privileges due to Improper Link Resolution via registry keys. This could enable a user with lower privileges to execute unauthorized tasks. **CVE ID : CVE-2023-24577**	https://www.mcafee.com/en-us/consumer-corporate/mcafee-labs/product-security-bulletins.html, https://www.mcafee.com/support/?articleId=TS103397&page=shell&shell=article-view	A-MCA-TOTA-280323/441
Affected Version(s): * Up to (excluding) 16.0.51					
N/A	13-Mar-2023	5.5	McAfee Total Protection prior to 16.0.51 allows attackers to trick a victim into uninstalling the application via the command prompt. **CVE ID : CVE-2023-24579**	https://www.mcafee.com/en-us/consumer-corporate/mcafee-labs/product-security-bulletins.html, https://www.mcafee.com/support/?articleId=TS103397&page=shell&shell=article-view	A-MCA-TOTA-280323/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: meddatapacs					
Product: meddatapacs					
Affected Version(s): * Up to (excluding) 2022-03-03					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MedData Informatics MedDataPACS.This issue affects MedDataPACS : before 2023-03-03. **CVE ID : CVE-2023-0979**	N/A	A-MED-MEDD-280323/443
Vendor: Medtronic					
Product: interstim_x_clinician					
Affected Version(s): a51300					
Improper Authentication	01-Mar-2023	6.8	Medtronic identified that the Pelvic Health clinician apps, which are installed on the Smart Programmer mobile device, have a password vulnerability that requires a security update to fix. Not updating could potentially result in unauthorized control of the clinician therapy application, which has greater control over therapy parameters than the patient app. Changes still cannot be made outside of the	https://global.medtronic.com/xg-en/product-security/security-bulletins/pelvic-health-interstim-micro.html	A-MED-INTE-280323/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			established therapy parameters of the programmer. For unauthorized access to occur, an individual would need physical access to the Smart Programmer. **CVE ID : CVE-2023-25931**		
Product: micro_clinician					
Affected Version(s): a51200					
Improper Authentication	01-Mar-2023	6.8	Medtronic identified that the Pelvic Health clinician apps, which are installed on the Smart Programmer mobile device, have a password vulnerability that requires a security update to fix. Not updating could potentially result in unauthorized control of the clinician therapy application, which has greater control over therapy parameters than the patient app. Changes still cannot be made outside of the established therapy parameters of the programmer. For unauthorized access to occur, an individual would need physical access	https://global.medtronic.com/xg-en/product-security/security-bulletins/pelvic-health-interstim-micro.html	A-MED-MICR-280323/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the Smart Programmer. **CVE ID : CVE-2023-25931**		
Vendor: mendix					
Product: saml					
Affected Version(s): From (including) 1.16.4 Up to (excluding) 1.17.2					
Improper Authentication	14-Mar-2023	7.5	A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All Versions >= 1.16.4 < 1.17.2), Mendix SAML (Mendix 8 compatible) (All versions >= 2.2.0 < 2.2.3), Mendix SAML (Mendix 9 compatible, New Track) (All versions >= 3.1.9 < 3.2.5), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions >= 3.1.9 < 3.2.5). The affected versions of the module insufficiently verifies the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application. **CVE ID : CVE-2023-25957**	N/A	A-MEN-SAML-280323/446
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	14-Mar-2023	7.5	A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All Versions >= 1.16.4 < 1.17.2), Mendix SAML (Mendix 8 compatible) (All versions >= 2.2.0 < 2.2.3), Mendix SAML (Mendix 9 compatible, New Track) (All versions >= 3.1.9 < 3.2.5), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions >= 3.1.9 < 3.2.5). The affected versions of the module insufficiently verifies the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application. **CVE ID : CVE-2023-25957**	N/A	A-MEN-SAML-280323/447
Affected Version(s): From (including) 3.1.9 Up to (excluding) 3.2.5					
Improper Authentication	14-Mar-2023	7.5	A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All Versions >= 1.16.4 < 1.17.2), Mendix SAML (Mendix 8 compatible) (All	N/A	A-MEN-SAML-280323/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions >= 2.2.0 < 2.2.3), Mendix SAML (Mendix 9 compatible, New Track) (All versions >= 3.1.9 < 3.2.5), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions >= 3.1.9 < 3.2.5). The affected versions of the module insufficiently verifies the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application. **CVE ID : CVE-2023-25957**		
Vendor: metagauss					
Product: registrationmagic					
Affected Version(s): * Up to (excluding) 5.1.9.3					
Cross-Site Request Forgery (CSRF)	13-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in RegistrationMagic plugin <= 5.1.9.2 versions. **CVE ID : CVE-2023-25991**	N/A	A-MET-REGI-280323/449
Vendor: metersphere					
Product: metersphere					
Affected Version(s): * Up to (excluding) 1.20.19					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Mar-2023	7.5	metersphere is an open source continuous testing platform. In affected versions an improper access control vulnerability exists in `/api/jmeter/download/files`, which allows any user to download any file without authentication. This issue may expose all files available to the running process. This issue has been addressed in version 1.20.20 lts and 2.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-25573**	N/A	A-MET-METE-280323/450
Affected Version(s): * Up to (excluding) 2.7.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-Mar-2023	6.5	metersphere is an open source continuous testing platform. In versions prior to 2.7.1 a user who has permission to create a resource file through UI operations is able to append a path to their submission query which will be read by the system and displayed to the user. This allows a	N/A	A-MET-METE-280323/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users of the system to read arbitrary files on the filesystem of the server so long as the server process itself has permission to read the requested files. This issue has been addressed in version 2.7.1. All users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-25814**		
Affected Version(s): From (including) 2.0.0 Up to (including) 2.6.2					
Missing Authorization	09-Mar-2023	7.5	metersphere is an open source continuous testing platform. In affected versions an improper access control vulnerability exists in `/api/jmeter/download/files`, which allows any user to download any file without authentication. This issue may expose all files available to the running process. This issue has been addressed in version 1.20.20 lts and 2.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	A-MET-METE-280323/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25573		
Vendor: Microsoft					
Product: 365					
Affected Version(s): -					
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	A-MIC-365-280323/453
Product: 365_apps					
Affected Version(s): -					
Authentication Bypass by Capture-replay	14-Mar-2023	9.8	Microsoft Outlook Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23397**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397	A-MIC-365_-280323/454
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-365_-280323/455
N/A	14-Mar-2023	5.5	Microsoft Excel Spoofing Vulnerability **CVE ID : CVE-2023-23398**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23398	A-MIC-365_-280323/456
Product: azure_hdinsights					
Affected Version(s): -					
N/A	14-Mar-2023	4.5	Azure Apache Ambari Spoofing Vulnerability **CVE ID : CVE-2023-23408**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23408	A-MIC-AZUR-280323/457

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: azure_service_fabric					
Affected Version(s): 9.1					
N/A	14-Mar-2023	5.4	Service Fabric Explorer Spoofing Vulnerability **CVE ID : CVE-2023-23383**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23383	A-MIC-AZUR-280323/458
Product: azure_setup_kubectl					
Affected Version(s): * Up to (excluding) 3.0					
Incorrect Permission Assignment for Critical Resource	06-Mar-2023	7	Azure/setup-kubectl is a GitHub Action for installing Kubectl. This vulnerability only impacts versions before version 3. An insecure temporary creation of a file allows other actors on the Actions runner to replace the Kubectl binary created by this action because it is world writable. This Kubectl tool installer runs `fs.chmodSync(kubectlPath, 777)` to set permissions on the Kubectl binary, however, this allows any local user to replace the Kubectl binary. This allows privilege escalation to the user that can also run kubectl, most likely root. This attack is only possible if an	https://github.com/Azure/setup-kubectl/security/advisories/GHSA-p756-rfxh-x63h, https://github.com/Azure/setup-kubectl/commit/d449d75495d2b9d1463555bb00ca3dca77a42ab6	A-MIC-AZUR-280323/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker somehow breached the GitHub actions runner or if a user is utilizing an Action that maliciously executes this attack. This has been fixed and released in all versions `v3` and later. 775 permissions are used instead. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-23939**		
Product: dynamics_365					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.0.45.11					
N/A	14-Mar-2023	7.5	Microsoft Dynamics 365 Information Disclosure Vulnerability **CVE ID : CVE-2023-24922**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24922	A-MIC-DYNA-280323/460
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24879**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24879	A-MIC-DYNA-280323/461
Improper Neutralization of Input During Web Page	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-DYNA-280323/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-24891**	ability/CVE-2023-24891	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24919**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24919	A-MIC-DYNA-280323/463
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24920**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24920	A-MIC-DYNA-280323/464
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24921**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24921	A-MIC-DYNA-280323/465
Affected Version(s): From (including) 9.1 Up to (excluding) 9.1.16.20					
N/A	14-Mar-2023	7.5	Microsoft Dynamics 365 Information Disclosure Vulnerability **CVE ID : CVE-2023-24922**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24922	A-MIC-DYNA-280323/466
Improper Neutralization of Input During	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-DYNA-280323/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-24879**	ability/CVE-2023-24879	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24891**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24891	A-MIC-DYNA-280323/468
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24919**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24919	A-MIC-DYNA-280323/469
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24920**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24920	A-MIC-DYNA-280323/470
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability **CVE ID : CVE-2023-24921**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24921	A-MIC-DYNA-280323/471
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 111.0.1661.41					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	14-Mar-2023	4.7	Microsoft Edge (Chromium-based) Webview2 Spoofing Vulnerability **CVE ID : CVE-2023-24892**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24892	A-MIC-EDGE-280323/472
Product: excel					
Affected Version(s): 2013					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-EXCE-280323/473
N/A	14-Mar-2023	5.5	Microsoft Excel Spoofing Vulnerability **CVE ID : CVE-2023-23398**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23398	A-MIC-EXCE-280323/474
Affected Version(s): 2016					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-EXCE-280323/475
N/A	14-Mar-2023	5.5	Microsoft Excel Spoofing Vulnerability **CVE ID : CVE-2023-23398**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23398	A-MIC-EXCE-280323/476
Product: malware_protection_engine					
Affected Version(s): 1.1.20000.2					
N/A	14-Mar-2023	6.3	Microsoft Defender Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-MALW-280323/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23389	ability/CVE-2023-23389	
Product: office					
Affected Version(s): -					
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	A-MIC-OFFI-280323/478
Affected Version(s): 2013					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-OFFI-280323/479
Affected Version(s): 2016					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-OFFI-280323/480
Affected Version(s): 16.0.16026.20172					
N/A	14-Mar-2023	5.5	Office for Android Spoofing Vulnerability **CVE ID : CVE-2023-23391**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23391	A-MIC-OFFI-280323/481
Affected Version(s): 2019					
Authentication Bypass by Capture-replay	14-Mar-2023	9.8	Microsoft Outlook Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23397**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397	A-MIC-OFFI-280323/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-OFFI-280323/483
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	A-MIC-OFFI-280323/484
N/A	14-Mar-2023	5.5	Microsoft Excel Spoofing Vulnerability **CVE ID : CVE-2023-23398**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23398	A-MIC-OFFI-280323/485
Affected Version(s): 2021					
Authentication Bypass by Capture-replay	14-Mar-2023	9.8	Microsoft Outlook Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23397**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397	A-MIC-OFFI-280323/486
N/A	14-Mar-2023	5.5	Microsoft Excel Spoofing Vulnerability **CVE ID : CVE-2023-23398**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23398	A-MIC-OFFI-280323/487
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-OFFI-280323/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	A-MIC-OFFI-280323/489
Product: office_online_server					
Affected Version(s): -					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-OFFI-280323/490
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Microsoft Excel Denial of Service Vulnerability **CVE ID : CVE-2023-23396**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23396	A-MIC-OFFI-280323/491
Product: office_web_apps_server					
Affected Version(s): 2013					
N/A	14-Mar-2023	7.8	Microsoft Excel Remote Code Execution Vulnerability **CVE ID : CVE-2023-23399**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399	A-MIC-OFFI-280323/492
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Microsoft Excel Denial of Service Vulnerability **CVE ID : CVE-2023-23396**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23396	A-MIC-OFFI-280323/493
Product: onedrive					
Affected Version(s): * Up to (excluding) 6.73					
N/A	14-Mar-2023	5.5	Microsoft OneDrive for Android Information	https://msrc.microsoft.com/update-	A-MIC-ONED-280323/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24923**	guide/vulnerability/CVE-2023-24923	
Affected Version(s): From (including) 1.0 Up to (excluding) 6.73					
N/A	14-Mar-2023	5.5	Microsoft OneDrive for Android Information Disclosure Vulnerability **CVE ID : CVE-2023-24882**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24882	A-MIC-ONED-280323/495
Affected Version(s): From (including) 1.0.0 Up to (excluding) 14.2.2					
N/A	14-Mar-2023	6.5	Microsoft OneDrive for iOS Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24890**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24890	A-MIC-ONED-280323/496
Affected Version(s): From (including) 22.0.0.0 Up to (excluding) 23.020.0125.0002					
N/A	14-Mar-2023	7.8	Microsoft OneDrive for MacOS Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24930**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24930	A-MIC-ONED-280323/497
Product: outlook					
Affected Version(s): 2013					
Authentication Bypass by Capture-replay	14-Mar-2023	9.8	Microsoft Outlook Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23397**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397	A-MIC-OUTL-280323/498
Affected Version(s): 2016					
Authentication Bypass by	14-Mar-2023	9.8	Microsoft Outlook Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-OUTL-280323/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Capture-replay			**CVE ID : CVE-2023-23397**	ability/CVE-2023-23397	
Product: sharepoint_foundation					
Affected Version(s): 2013					
N/A	14-Mar-2023	3.1	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-23395**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23395	A-MIC-SHAR-280323/500
Product: sharepoint_server					
Affected Version(s): -					
N/A	14-Mar-2023	3.1	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-23395**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23395	A-MIC-SHAR-280323/501
Affected Version(s): 2013					
N/A	14-Mar-2023	3.1	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-23395**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23395	A-MIC-SHAR-280323/502
Affected Version(s): 2019					
N/A	14-Mar-2023	3.1	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-23395**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23395	A-MIC-SHAR-280323/503
Vendor: minio					
Product: minio					
Affected Version(s): From (including) 2020-12-23t02-24-12z Up to (excluding) 2023-03-13t19-46-17z					
N/A	14-Mar-2023	6.5	Minio is a Multi-Cloud Object Storage framework. Starting	https://github.com/minio/minio/pull/	A-MIN-MINI-280323/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with RELEASE.2020-12-23T02-24-12Z and prior to RELEASE.2023-03-13T19-46-17Z, a user with `consoleAdmin` permissions can potentially create a user that matches the root credential `accessKey`. Once this user is created successfully, the root credential ceases to work appropriately. The issue is patched in RELEASE.2023-03-13T19-46-17Z. There are ways to work around this via adding higher privileges to the disabled root user via `mc admin policy set`. **CVE ID : CVE-2023-27589**	16803, https://github.com/minio/minio/security/advisories/GHSA-9wfv-wmf7-6753	
Vendor: mobyproject					
Product: buildkit					
Affected Version(s): From (including) 0.10.0 Up to (excluding) 0.11.4					
N/A	06-Mar-2023	6.5	BuildKit is a toolkit for converting source code to build artifacts in an efficient, expressive and repeatable manner. In affected versions when the user sends a build request that contains a Git URL that	https://github.com/moby/buildkit/commit/75123c696506bdbca1ed69906479e200f1b62604, https://github.com/moby/buildkit/se	A-MOB-BUIL-280323/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains credentials and the build creates a provenance attestation describing that build, these credentials could be visible from the provenance attestation. Git URL can be passed in two ways: 1) Invoking build directly from a URL with credentials. 2) If the client sends additional version control system (VCS) info hint parameters on builds from a local source. Usually, that would mean reading the origin URL from `.git/config` file. When a build is performed under specific conditions where credentials were passed to BuildKit they may be visible to everyone who has access to provenance attestation. Provenance attestations and VCS info hints were added in version v0.11.0. Previous versions are not vulnerable. In v0.10, when building directly from Git URL, the same URL	curity/advisories/GHSA-gc89-7gcr-jxqc	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be visible in `BuildInfo` structure that is a predecessor of Provenance attestations. Previous versions are not vulnerable. This bug has been fixed in v0.11.4. Users are advised to upgrade. Users unable to upgrade may disable VCS info hints by setting `BUILDX_GIT_INFO=0`. `buildctl` does not set VCS hints based on `.git` directory, and values would need to be passed manually with `--opt`. **CVE ID : CVE-2023-26054**		
Vendor: monospace					
Product: directus					
Affected Version(s): * Up to (excluding) 9.16.0					
Exposure of Sensitive Information to an Unauthorized Actor	07-Mar-2023	4.3	Directus is a real-time API and App dashboard for managing SQL database content. In versions prior to 9.16.0 users with read access to the `password` field in `directus_users` can extract the argon2 password hashes by brute forcing the export functionality combined with a	https://github.com/directus/directus/pull/15010, https://github.com/directus/directus/pull/14829, https://github.com/directus/directus/security/advisories/GHSA-m5q3-8wgf-x8xf	A-MON-DIRE-280323/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`_starts_with` filter. This allows the user to enumerate the password hashes. Accounts cannot be taken over unless the hashes can be reversed which is unlikely with current hardware. This problem has been patched by preventing any hashed/concealed field to be filtered against with the `_starts_with` or other string operator in version 9.16.0. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by ensuring that no user has `read` access to the `password` field in `directus_users`. **CVE ID : CVE-2023-27481**		
Affected Version(s): * Up to (excluding) 9.23.0					
Server-Side Request Forgery (SSRF)	03-Mar-2023	7.5	Directus is a real-time API and App dashboard for managing SQL database content. Directus is vulnerable to Server-Side Request Forgery (SSRF) when importing a file from a remote web server (POST to	https://github.com/directus/directus/commit/ff53d3e69a602d05342e15d9bb616884833ddbff	A-MON-DIRE-280323/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`/files/import`). An attacker can bypass the security controls by performing a DNS rebinding attack and view sensitive data from internal servers or perform a local port scan. An attacker can exploit this vulnerability to access highly sensitive internal server(s) and steal sensitive information. This issue was fixed in version 9.23.0. **CVE ID : CVE-2023-26492**		
Vendor: moosikay_project					
Product: moosikay					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	9.8	E-Commerce System v1.0 ws discovered to contain a SQL injection vulnerability via the id parameter at /admin/delete_user.php. **CVE ID : CVE-2023-27052**	N/A	A-MOO-MOOS-280323/508
Vendor: my-blog_project					
Product: my-blog					
Affected Version(s): -					
Improper Neutralization of Input During	13-Mar-2023	6.1	Cross Site Scripting vulnerability found in My-Blog allows attackers to cause a	N/A	A-MY--MY-B-280323/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			denial of service via the Post function. **CVE ID : CVE-2023-27093**		
Vendor: nestjs					
Product: nest					
Affected Version(s): * Up to (excluding) 9.0.5					
N/A	06-Mar-2023	5.3	Versions of the package @nestjs/core before 9.0.5 are vulnerable to Information Exposure via the StreamableFile pipe. Exploiting this vulnerability is possible when the client cancels a request while it is streaming a StreamableFile, the stream wrapped by the StreamableFile will be kept open. **CVE ID : CVE-2023-26108**	https://github.com/nestjs/nest/pull/9819/commits/f59cf5e81ca73bcdf1b5b36713550fd93918db41, https://github.com/nestjs/nest/pull/9819	A-NES-NEST-280323/510
Vendor: Netiq					
Product: advanced_authentication					
Affected Version(s): From (including) 6.3.0.0 Up to (excluding) 6.3.7.2					
N/A	15-Mar-2023	9.8	Broken access control in Advanced Authentication versions prior to 6.4.1.1 and 6.3.7.2 **CVE ID : CVE-2023-24468**	N/A	A-NET-ADVA-280323/511
Affected Version(s): From (including) 6.4.0.0 Up to (excluding) 6.4.1.1					
N/A	15-Mar-2023	9.8	Broken access control in Advanced	N/A	A-NET-ADVA-280323/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Authentication versions prior to 6.4.1.1 and 6.3.7.2 **CVE ID : CVE-2023-24468**		
Vendor: nextauth.js					
Product: next-auth					
Affected Version(s): * Up to (excluding) 4.20.1					
Cross-Site Request Forgery (CSRF)	09-Mar-2023	8.8	NextAuth.js is an open source authentication solution for Next.js applications. `next-auth` applications using OAuth provider versions before `v4.20.1` have been found to be subject to an authentication vulnerability. A bad actor who can read traffic on the victim's network or who is able to social engineer the victim to click a manipulated login link could intercept and tamper with the authorization URL to **log in as the victim**, bypassing the CSRF protection. This is due to a partial failure during a compromised OAuth session where a session code is erroneously generated. This issue has been addressed	https://github.com/nextauthjs/next-auth/security/advisories/GHSA-7r7x-4c4q-c4qf	A-NEX-NEXT-280323/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in version 4.20.1. Users are advised to upgrade. Users unable to upgrade may using Advanced Initialization, manually check the callback request for state, pkce, and nonce against the provider configuration to prevent this issue. See the linked GHSA for details. **CVE ID : CVE-2023-27490**		
Vendor: nicdark					
Product: cost_calculator					
Affected Version(s): * Up to (including) 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The Cost Calculator WordPress plugin through 1.8 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0165**	N/A	A-NIC-COST-280323/514
Improper Neutralization of Input	02-Mar-2023	5.4	The Cost Calculator plugin for WordPress is vulnerable to Stored	N/A	A-NIC-COST-280323/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting via the nd_cc_meta_box_cc_price_icon parameter in versions up to, and including, 1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-1155**		
Vendor: nistec_project					
Product: nistec					
Affected Version(s): * Up to (excluding) 0.0.2					
Incorrect Calculation	08-Mar-2023	7.5	Multiplication of certain unreduced P-256 scalars produce incorrect results. There are no protocols known at this time that can be attacked due to this. **CVE ID : CVE-2023-24533**	https://github.com/FiloSottile/nistec/commit/c58aa1223ccf3943513e1e661cebce95af137244, https://go.dev/issue/58647	A-NIS-NIST-280323/516
Vendor: niteothemes					
Product: coming_soon_\&_maintenance					
Affected Version(s): * Up to (including) 4.1.6					
Exposure of Sensitive	07-Mar-2023	5.3	The CMP – Coming Soon & Maintenance	https://plugins.trac.word	A-NIT-COMI-280323/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			plugin for WordPress is vulnerable to Information Exposure in versions up to, and including, 4.1.6 via the cmp_get_post_detail function. This can allow unauthenticated individuals to obtain the contents of any non-password-protected, published post or page even when maintenance mode is enabled. **CVE ID : CVE-2023-1263**	press.org/browser/cmp-coming-soon-maintenance/tags/4.1.6/niteo-cmp.php#L2759	
Vendor: node-bluetooth-serial-port_project					
Product: node-bluetooth-serial-port					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-Mar-2023	9.8	All versions of the package node-bluetooth-serial-port are vulnerable to Buffer Overflow via the findSerialPortChannel method due to improper user input length validation. **CVE ID : CVE-2023-26109**	N/A	A-NOD-NODE-280323/518
Vendor: node-bluetooth_project					
Product: node-bluetooth					
Affected Version(s): * Up to (including) 1.2.6					
Buffer Copy without	09-Mar-2023	9.8	All versions of the package node-bluetooth are	N/A	A-NOD-NODE-280323/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			vulnerable to Buffer Overflow via the findSerialPortChannel method due to improper user input length validation. **CVE ID : CVE-2023-26110**		
Vendor: node-static_project					
Product: node-static					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Mar-2023	7.5	All versions of the package @nubosoftware/node-static; all versions of the package node-static are vulnerable to Directory Traversal due to improper file path sanitization in the startsWith() method in the servePath function. **CVE ID : CVE-2023-26111**	N/A	A-NOD-NODE-280323/520
Vendor: Nvidia					
Product: cuda_toolkit					
Affected Version(s): * Up to (excluding) 12.1					
Out-of-bounds Read	10-Mar-2023	4.4	NVIDIA CUDA Toolkit SDK contains a vulnerability in cuobjdump, where a local user running the tool against a malicious binary may cause an out-of-bounds read, which may result in a limited denial of service and limited	https://nvidia.custhelp.com/app/answers/detail/a_id/5446	A-NVI-CUDA-280323/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2023-0193**		
NULL Pointer Dereference	02-Mar-2023	3.3	NVIDIA CUDA Toolkit SDK contains a bug in cuobjdump, where a local user running the tool against an ill-formed binary may cause a null- pointer dereference, which may result in a limited denial of service. **CVE ID : CVE-2023-0196**	https://nvidia.custhelp.com/app/answers/detail/a_id/5446	A-NVI-CUDA-280323/522
Vendor: oceanwp					
Product: ocean_extra					
Affected Version(s): * Up to (excluding) 2.1.3					
N/A	13-Mar-2023	6.5	The Ocean Extra WordPress plugin before 2.1.3 does not ensure that the template to be loaded via a shortcode is actually a template, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, such as draft, private or even password protected ones. **CVE ID : CVE-2023-0749**	N/A	A-OCE-OCEA-280323/523
Vendor: okta					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: advanced_server_access					
Affected Version(s): From (including) 1.13.1 Up to (excluding) 1.68.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Mar-2023	8.8	Okta Advanced Server Access Client versions 1.13.1 through 1.65.0 are vulnerable to command injection due to the third party library webbrowser. An outdated library, webbrowser, used by the ASA client was found to be vulnerable to command injection. To exploit this issue, an attacker would need to phish the user to enter an attacker controlled server URL during enrollment. **CVE ID : CVE-2023-0093**	https://trust.okta.com/security-advisories/okta-advanced-server-access-client-cve-2023-0093/	A-OKT-ADVA-280323/524
Vendor: onekeyadmin					
Product: onekeyadmin					
Affected Version(s): 1.3.9					
Unrestricted Upload of File with Dangerous Type	06-Mar-2023	9.8	An arbitrary file upload vulnerability in the component /admin1/config/update of onekeyadmin v1.3.9 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2023-26949**	N/A	A-ONE-ONEK-280323/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Mar-2023	9.1	onekeyadmin v1.3.9 was discovered to contain an arbitrary file delete vulnerability via the component \admin\controller\plugins. **CVE ID : CVE-2023-26957**	N/A	A-ONE-ONEK-280323/526
Files or Directories Accessible to External Parties	09-Mar-2023	7.5	onekeyadmin v1.3.9 was discovered to contain an arbitrary file read vulnerability via the component /admin1/file/download. **CVE ID : CVE-2023-26948**	N/A	A-ONE-ONEK-280323/527
Files or Directories Accessible to External Parties	08-Mar-2023	7.5	onekeyadmin v1.3.9 was discovered to contain an arbitrary file read vulnerability via the component /admin1/curd/code. **CVE ID : CVE-2023-26956**	N/A	A-ONE-ONEK-280323/528
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	5.4	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Title parameter under the Adding Categories module. **CVE ID : CVE-2023-26950**	N/A	A-ONE-ONEK-280323/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	5.4	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Menu module. **CVE ID : CVE-2023-26952**	N/A	A-ONE-ONEK-280323/530
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	4.8	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Add Administrator module. **CVE ID : CVE-2023-26953**	N/A	A-ONE-ONEK-280323/531
Vendor: onekeyadmin_project					
Product: onekeyadmin					
Affected Version(s): 1.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the User Group module. **CVE ID : CVE-2023-26954**	N/A	A-ONE-ONEK-280323/532
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	onekeyadmin v1.3.9 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Admin Group module. **CVE ID : CVE-2023-26955**	N/A	A-ONE-ONEK-280323/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 1.0					
Cross-Site Request Forgery (CSRF)	14-Mar-2023	6.5	A Cross-Site Request Forgery (CSRF) in Online Food Ordering System v1.0 allows attackers to change user details and credentials via a crafted POST request. **CVE ID : CVE-2023-27073**	N/A	A-ONL-ONLI-280323/534
Vendor: online_graduate_tracer_system_project					
Product: online_graduate_tracer_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. This issue affects the function mysqli_query of the file admin_cs.php. The manipulation leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222647. **CVE ID : CVE-2023-1293**	N/A	A-ONL-ONLI-280323/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file admin/adminlog.php. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222696. **CVE ID : CVE-2023-1308**	N/A	A-ONL-ONLI-280323/536
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Graduate Tracer System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/search_it.php. The manipulation of the argument input leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the	N/A	A-ONL-ONLI-280323/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The identifier VDB-222697 was assigned to this vulnerability. **CVE ID : CVE-2023-1309**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Graduate Tracer System 1.0. Affected by this issue is some unknown functionality of the file admin/prof.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-222698 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1310**	N/A	A-ONL-ONLI-280323/538
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	9.8	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been classified as critical. This affects the function mysqli_query of the file bsitemp.php. The manipulation of the	N/A	A-ONL-ONLI-280323/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222981 was assigned to this vulnerability. **CVE ID : CVE-2023-1394**		
Vendor: online_pizza_ordering_system_project					
Product: online_pizza_ordering_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	14-Mar-2023	9.8	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is the function save_menu. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222979. **CVE ID : CVE-2023-1392**	N/A	A-ONL-ONLI-280323/540
Improper Neutralization of	09-Mar-2023	9.8	Online Pizza Ordering System 1.0 was discovered to	N/A	A-ONL-ONLI-280323/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			contain a SQL injection vulnerability via the id parameter at /admin/manage_user.php. **CVE ID : CVE-2023-27207**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Online Pizza Ordering System 1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/view_order.php. **CVE ID : CVE-2023-27210**	N/A	A-ONL-ONLI-280323/542
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	7.5	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file category.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-ONL-ONLI-280323/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-222871. **CVE ID : CVE-2023-1364**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	7.5	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/ajax.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222872. **CVE ID : CVE-2023-1365**	N/A	A-ONL-ONLI-280323/544
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in /php-opos/login.php of Online Pizza Ordering System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the redirect parameter. **CVE ID : CVE-2023-27208**	N/A	A-ONL-ONLI-280323/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in /admin/navbar.php of Online Pizza Ordering System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the page parameter. **CVE ID : CVE-2023-27211**	N/A	A-ONL-ONLI-280323/546
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in /php-opos/signup.php of Online Pizza Ordering System 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the redirect parameter. **CVE ID : CVE-2023-27212**	N/A	A-ONL-ONLI-280323/547
Vendor: online_student_management_system_project					
Product: online_student_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Online Student Management System v1.0 was discovered to contain a SQL injection vulnerability via the searchdata parameter at /eduauth/student/search.php.	N/A	A-ONL-ONLI-280323/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27213		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	Online Student Management System v1.0 was discovered to contain multiple SQL injection vulnerabilities via the fromdate and todate parameters at /eduauth/student/between-date-reprtsdetails.php. **CVE ID : CVE-2023-27214**	N/A	A-ONL-ONLI-280323/549
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Online Student Management System 1.0. Affected is an unknown function of the file profile.php. The manipulation of the argument adminname leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222984. **CVE ID : CVE-2023-1397**	N/A	A-ONL-ONLI-280323/550
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	14-Mar-2023	9.8	A vulnerability, which was classified as problematic, was found in SourceCodester Online Tours & Travels Management System 1.0. Affected is an unknown function of the file admin/ab.php. The manipulation of the argument img leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222978 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1391**	N/A	A-ONL-ONLI-280323/551
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file admin/traveller_details.php. The manipulation of the argument address leads to cross site scripting. The attack	N/A	A-ONL-ONLI-280323/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222983. **CVE ID : CVE-2023-1396**		
Vendor: opendoas_project					
Product: opendoas					
Affected Version(s): * Up to (including) 6.8.2					
N/A	14-Mar-2023	8.8	OpenDoas through 6.8.2, when TIOCSTI is available, allows privilege escalation because of sharing a terminal with the original session. NOTE: TIOCSTI is unavailable in OpenBSD 6.0 and later, and can be made unavailable in the Linux kernel 6.2 and later. **CVE ID : CVE-2023-28339**	N/A	A-OPE-OPEN-280323/553
Vendor: openharmony					
Product: openharmony					
Affected Version(s): From (including) 3.0 Up to (including) 3.0.7					
Access of Resource Using Incompatible Type ('Type Confusion')	10-Mar-2023	5.5	The ArKUI framework subsystem within OpenHarmony-v3.1.5 and prior versions, OpenHarmony-v3.0.7 and prior versions has an	N/A	A-OPE-OPEN-280323/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Improper Input Validation vulnerability which local attackers can exploit this vulnerability to send malicious data, causing the current application to crash. **CVE ID : CVE-2023-0083**		
NULL Pointer Dereference	10-Mar-2023	5.5	Communication Wi-Fi subsystem within OpenHarmony-v3.1.4 and prior versions, OpenHarmony-v3.0.7 and prior versions has a null pointer reference vulnerability which local attackers can exploit this vulnerability to cause the current application to crash. **CVE ID : CVE-2023-24465**	N/A	A-OPE-OPEN-280323/555
Affected Version(s): From (including) 3.1 Up to (including) 3.1.4					
NULL Pointer Dereference	10-Mar-2023	5.5	Communication Wi-Fi subsystem within OpenHarmony-v3.1.4 and prior versions, OpenHarmony-v3.0.7 and prior versions has a null pointer reference vulnerability which local attackers can exploit this vulnerability to	N/A	A-OPE-OPEN-280323/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause the current application to crash. **CVE ID : CVE-2023-24465**		
Improper Input Validation	10-Mar-2023	5.5	The bundle management subsystem within OpenHarmony-v3.1.4 and prior versions has a null pointer reference vulnerability which local attackers can exploit this vulnerability to cause a DoS attack to the system when installing a malicious HAP package. **CVE ID : CVE-2023-25947**	N/A	A-OPE-OPEN-280323/557
Affected Version(s): From (including) 3.1 Up to (including) 3.1.5					
Use After Free	10-Mar-2023	7.8	The kernel subsystem function check_permission_for_set_tokenid within OpenHarmony-v3.1.5 and prior versions has an UAF vulnerability which local attackers can exploit this vulnerability to escalate the privilege to root. **CVE ID : CVE-2023-22436**	N/A	A-OPE-OPEN-280323/558
N/A	10-Mar-2023	7.5	The kernel subsystem hmdfs within OpenHarmony-v3.1.5 and prior	N/A	A-OPE-OPEN-280323/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions has an arbitrary memory accessing vulnerability which network attackers can launch a remote attack to obtain kernel memory data of the target system. **CVE ID : CVE-2023-22301**		
Access of Resource Using Incompatible Type ('Type Confusion')	10-Mar-2023	5.5	The ArKUI framework subsystem within OpenHarmony-v3.1.5 and prior versions, OpenHarmony-v3.0.7 and prior versions has an Improper Input Validation vulnerability which local attackers can exploit this vulnerability to send malicious data, causing the current application to crash. **CVE ID : CVE-2023-0083**	N/A	A-OPE-OPEN-280323/560
Vendor: opennetworking					
Product: onos					
Affected Version(s): From (including) 1.9.0 Up to (including) 2.7.0					
Improper Neutralization of Input During Web Page Generation	14-Mar-2023	6.1	A cross-site scripting (XSS) vulnerability in Open Networking Foundation ONOS from version v1.9.0 to v2.7.0 allows attackers to execute arbitrary web scripts	N/A	A-OPE-ONOS-280323/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			or HTML via a crafted payload injected into the url parameter of the API documentation dashboard. **CVE ID : CVE-2023-24279**		
Vendor: opensips					
Product: opensips					
Affected Version(s): * Up to (excluding) 3.1.7					
Use of Uninitialized Resource	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, sending a malformed `Via` header to OpenSIPS triggers a segmentation fault when the function `calc_tag_suffix` is called. A specially crafted `Via` header, which is deemed correct by the parser, will pass uninitialized strings to the function `MD5StringArray` which leads to the crash. Abuse of this vulnerability leads to Denial of Service due to a crash. Since the uninitialized string points to memory location `0x0`, no further exploitation appears to be possible. No special	https://github.com/OpenSIPS/opensips/commit/ab611f74f69d9c42be5401c40d56ea06a58f5dd7	A-OPE-OPEN-280323/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network privileges are required to perform this attack, as long as the OpenSIPS configuration makes use of functions such as `sl_send_reply` or `sl_gen_totag` that trigger the vulnerable code. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27598**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, when the function `append_hf` handles a SIP message with a malformed To header, a call to the function `abort()` is performed, resulting in a crash. This is due to the following check in `data_lump.c:399` in the function `anchor_lump`. An attacker abusing this vulnerability will crash OpenSIPS leading to Denial of Service. It affects configurations containing functions that make use of the	https://github.com/OpenSIPS/opensips/commit/cb56694d290530ac308f44b453c18120b1c1109d	A-OPE-OPEN-280323/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected code, such as the function `append_hf`. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27599**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received and is processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate by a line feed (i.e. `\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing	https://github.com/OpenSIPS/opensips/commit/c6ab3bb406c447e30c7d33a1a8970048b4612100, https://opensips.org/docs/modules/3.3.x/sipmsgops.html, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	A-OPE-OPEN-280323/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			coverage guided fuzzing on the function `codec_delete_except_re`. The crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\n`). By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is performed in the `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue is patched in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27600**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4,	https://github.com/OpenSIPS/opensips/commit/8f87c7c03da55f9c79bd9	A-OPE-OPEN-280323/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OpenSIPS crashes when a malformed SDP body is received and is processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate by a line feed (i.e. `\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_except_re`. The crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\n`): By abusing this vulnerability, an attacker is able to crash the server. It	2e67fa2c94b2a7ce5cf, https://opensips.org/docs/modules/3.3.x/sipmsgops.html, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is performed in the `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27601**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions prior to 3.1.7 and 3.2.4 have a potential issue in `msg_translator.c:2628` which might lead to a server crash. This issue was found while fuzzing the function `build_res_buf_from_sip_req` but could not be reproduced against a running instance of OpenSIPS. This issue could not be exploited against a	https://github.com/OpenSIPS/opensips/commit/9cf3dd3398719dd91207495f76d7726701c5145c, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	A-OPE-OPEN-280323/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running instance of OpenSIPS since no public function was found to make use of this vulnerable code. Even in the case of exploitation through unknown vectors, it is highly unlikely that this issue would lead to anything other than Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-28095**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, a specially crafted Authorization header causes OpenSIPS to crash or behave in an unexpected way due to a bug in the function `parse_param_name()` . This issue was discovered while performing coverage guided fuzzing of the function parse_msg. The AddressSanitizer identified that the issue occurred in the function `q_memchr()` which is being called by the	https://github.com/OpenSIPS/opensips/commit/dd9141b6f67d7df4072f3430f628d4b73df5e102	A-OPE-OPEN-280323/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function `parse_param_name()`. This issue may cause erratic program behaviour or a server crash. It affects configurations containing functions that make use of the affected code, such as the function `www_authorize()` . Versions 3.1.7 and 3.2.4 contain a fix. **CVE ID : CVE-2023-28098**		
Affected Version(s): * Up to (excluding) 3.1.8					
Allocation of Resources Without Limits or Throttling	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, OpenSIPS crashes when a malformed SDP body is sent multiple times to an OpenSIPS configuration that makes use of the `stream_process` function. This issue was discovered during coverage guided fuzzing of the function `codec_delete_except_re`. By abusing this vulnerability, an attacker is able to crash the server. It affects	https://github.com/OpenSIPS/opensips/commit/dd051f8ed5ae3347fb1d556ced3c97822c9d8450	A-OPE-OPEN-280323/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. This issue has been fixed in version 3.1.8 and 3.2.5. **CVE ID : CVE-2023-27596**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, when a specially crafted SIP message is processed by the function `rewrite_ruri`, a crash occurs due to a segmentation fault. This issue causes the server to crash. It affects configurations containing functions that make use of the affected code, such as the function `setport`. This issue has been fixed in version 3.1.8 and 3.2.5. **CVE ID : CVE-2023-27597**	https://github.com/OpenSIPS/opensips/commit/b2dffe4b5cd81182c9c8eabb6c96aac96c7acfe3	A-OPE-OPEN-280323/569
Missing Release of Memory after	15-Mar-2023	7.5	OpenSIPS, a Session Initiation Protocol (SIP) server implementation, has a memory leak	https://github.com/OpenSIPS/opensips/commit/4175687075	A-OPE-OPEN-280323/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			starting in the 2.3 branch and priot to versions 3.1.8 and 3.2.5. The memory leak was detected in the function `parse_mi_request` while performing coverage-guided fuzzing. This issue can be reproduced by sending multiple requests of the form `{"jsonrpc": "2.0","method": "log_le`. This malformed message was tested against an instance of OpenSIPS via FIFO transport layer and was found to increase the memory consumption over time. To abuse this memory leak, attackers need to reach the management interface (MI) which typically should only be exposed on trusted interfaces. In cases where the MI is exposed to the internet without authentication, abuse of this issue will lead to memory exhaustion which may affect the underlying system's availability. No authentication is	20af25ec5c5dd91da18e6db3649dcb, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically required to reproduce this issue. On the other hand, memory leaks may occur in other areas of OpenSIPS where the cJSON library is used for parsing JSON objects. The issue has been fixed in versions 3.1.8 and 3.2.5. **CVE ID : CVE-2023-28096**		
Affected Version(s): * Up to (excluding) 3.1.9					
Integer Overflow or Wraparound	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, a malformed SIP message containing a large _Content-Length_ value and a specially crafted Request-URI causes a segmentation fault in OpenSIPS. This issue occurs when a large amount of shared memory using the `-m` flag was allocated to OpenSIPS, such as 10 GB of RAM. On the test system, this issue occurred when shared memory was set to `2362` or higher. This issue is fixed in versions 3.1.9 and 3.2.6. The	https://github.com/OpenSIPS/opensips/commit/7cab422e2fc648f910abba34f3f0dbb3ae171ff5, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	A-OPE-OPEN-280323/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only workaround is to guarantee that the Content-Length value of input messages is never larger than `2147483647`. **CVE ID : CVE-2023-28097**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, if `ds_is_in_list()` is used with an invalid IP address string (`NULL` is illegal input), OpenSIPS will attempt to print a string from a random address (stack garbage), which could lead to a crash. All users of `ds_is_in_list()` without the `$si` variable as 1st parameter could be affected by this vulnerability to a larger, lesser or no extent at all, depending if the data passed to the function is a valid IPv4 or IPv6 address string or not. Fixes will are available starting with the 3.1.9 and 3.2.6 minor releases. There are	https://github.com/OpenSIPS/opensips/commit/e2f13d374	A-OPE-OPEN-280323/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no known workarounds. **CVE ID : CVE-2023-28099**		
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.2.4					
Use of Uninitialized Resource	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, sending a malformed `Via` header to OpenSIPS triggers a segmentation fault when the function `calc_tag_suffix` is called. A specially crafted `Via` header, which is deemed correct by the parser, will pass uninitialized strings to the function `MD5StringArray` which leads to the crash. Abuse of this vulnerability leads to Denial of Service due to a crash. Since the uninitialized string points to memory location `0x0`, no further exploitation appears to be possible. No special network privileges are required to perform this attack, as long as the OpenSIPS configuration makes use of functions such	https://github.com/OpenSIPS/opensips/commit/ab611f74f69d9c42be5401c40d56ea06a58f5dd7	A-OPE-OPEN-280323/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as `sl_send_reply` or `sl_gen_totag` that trigger the vulnerable code. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27598**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, when the function `append_hf` handles a SIP message with a malformed To header, a call to the function `abort()` is performed, resulting in a crash. This is due to the following check in `data_lump.c:399` in the function `anchor_lump`. An attacker abusing this vulnerability will crash OpenSIPS leading to Denial of Service. It affects configurations containing functions that make use of the affected code, such as the function `append_hf`. This issue has been fixed in versions 3.1.7 and 3.2.4.	https://github.com/OpenSIPS/opensips/commit/cb56694d290530ac308f44b453c18120b1c1109d	A-OPE-OPEN-280323/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27599		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received and is processed by the `delete_sdp_line` function in the sipmsgops module. This issue can be reproduced by calling the function with an SDP body that does not terminate by a line feed (i.e. `\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_except_re`. The crash happens because the function	https://github.com/OpenSIPS/opensips/commit/c6ab3bb406c447e30c7d33a1a8970048b4612100, https://opensips.org/docs/modules/3.3.x/sipmsgops.html, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	A-OPE-OPEN-280323/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`delete_sdp_line` expects that an SDP line is terminated by a line feed (`\n`). By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. Due to the sanity check that is performed in the `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue is patched in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27600**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, OpenSIPS crashes when a malformed SDP body is received and is processed by the `delete_sdp_line` function in the sipmsgops module.	https://github.com/OpenSIPS/opensips/commit/8f87c7c03da55f9c79bd92e67fa2c94b2a7ce5cf, https://opensips.org/docs/modules/3.3.x/sipmsgops.html,	A-OPE-OPEN-280323/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue can be reproduced by calling the function with an SDP body that does not terminate by a line feed (i.e. `\n`). The vulnerability was found while performing black-box fuzzing against an OpenSIPS server running a configuration that made use of the functions `codec_delete_except_re` and `codec_delete_re`. The same issue was also discovered while performing coverage guided fuzzing on the function `codec_delete_except_re`. The crash happens because the function `delete_sdp_line` expects that an SDP line is terminated by a line feed (`\n`): By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except	https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_re`. Due to the sanity check that is performed in the `del_lump` function, exploitation of this issue will generate an `abort` in the lumps processing function, resulting in a Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-27601**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions prior to 3.1.7 and 3.2.4 have a potential issue in `msg_translator.c:2628` which might lead to a server crash. This issue was found while fuzzing the function `build_res_buf_from_sip_req` but could not be reproduced against a running instance of OpenSIPS. This issue could not be exploited against a running instance of OpenSIPS since no public function was found to make use of this vulnerable code. Even in the case of exploitation through	https://github.com/OpenSIPS/opensips/commit/9cf3dd3398719dd91207495f76d7726701c5145c, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	A-OPE-OPEN-280323/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown vectors, it is highly unlikely that this issue would lead to anything other than Denial of Service. This issue has been fixed in versions 3.1.7 and 3.2.4. **CVE ID : CVE-2023-28095**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.7 and 3.2.4, a specially crafted Authorization header causes OpenSIPS to crash or behave in an unexpected way due to a bug in the function `parse_param_name()` . This issue was discovered while performing coverage guided fuzzing of the function parse_msg. The AddressSanitizer identified that the issue occurred in the function `q_memchr()` which is being called by the function `parse_param_name()`. This issue may cause erratic program behaviour or a server crash. It affects	https://github.com/OpenSIPS/opensips/commit/dd9141b6f67d7df4072f3430f628d4b73df5e102	A-OPE-OPEN-280323/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configurations containing functions that make use of the affected code, such as the function `www_authorize()` . Versions 3.1.7 and 3.2.4 contain a fix. **CVE ID : CVE-2023-28098**		
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.2.5					
Allocation of Resources Without Limits or Throttling	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, OpenSIPS crashes when a malformed SDP body is sent multiple times to an OpenSIPS configuration that makes use of the `stream_process` function. This issue was discovered during coverage guided fuzzing of the function `codec_delete_except_re`. By abusing this vulnerability, an attacker is able to crash the server. It affects configurations containing functions that rely on the affected code, such as the function `codec_delete_except_re`. This issue has	https://github.com/OpenSIPS/opensips/commit/dd051f8ed5ae3347fb1d556ced3c97822c9d8450	A-OPE-OPEN-280323/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been fixed in version 3.1.8 and 3.2.5. **CVE ID : CVE-2023-27596**		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.8 and 3.2.5, when a specially crafted SIP message is processed by the function `rewrite_ruri`, a crash occurs due to a segmentation fault. This issue causes the server to crash. It affects configurations containing functions that make use of the affected code, such as the function `setport`. This issue has been fixed in version 3.1.8 and 3.2.5. **CVE ID : CVE-2023-27597**	https://github.com/OpenSIPS/opensips/commit/b2dffe4b5cd81182c9c8eabb6c96aac96c7acfe3	A-OPE-OPEN-280323/580
Missing Release of Memory after Effective Lifetime	15-Mar-2023	7.5	OpenSIPS, a Session Initiation Protocol (SIP) server implementation, has a memory leak starting in the 2.3 branch and priot to versions 3.1.8 and 3.2.5. The memory leak was detected in the function `parse_mi_request`	https://github.com/OpenSIPS/opensips/commit/417568707520af25ec5c5dd91da18e6db3649dcb, https://opensips.org/pub/audit-2022/opensi	A-OPE-OPEN-280323/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while performing coverage-guided fuzzing. This issue can be reproduced by sending multiple requests of the form `{"jsonrpc": "2.0","method": "log_le`. This malformed message was tested against an instance of OpenSIPS via FIFO transport layer and was found to increase the memory consumption over time. To abuse this memory leak, attackers need to reach the management interface (MI) which typically should only be exposed on trusted interfaces. In cases where the MI is exposed to the internet without authentication, abuse of this issue will lead to memory exhaustion which may affect the underlying system's availability. No authentication is typically required to reproduce this issue. On the other hand, memory leaks may occur in other areas of OpenSIPS where the cJSON library is	ps-audit-technical-report-full.pdf	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used for parsing JSON objects. The issue has been fixed in versions 3.1.8 and 3.2.5. **CVE ID : CVE-2023-28096**		
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.2.6					
Integer Overflow or Wraparound	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, a malformed SIP message containing a large _Content-Length_ value and a specially crafted Request-URI causes a segmentation fault in OpenSIPS. This issue occurs when a large amount of shared memory using the `-m` flag was allocated to OpenSIPS, such as 10 GB of RAM. On the test system, this issue occurred when shared memory was set to `2362` or higher. This issue is fixed in versions 3.1.9 and 3.2.6. The only workaround is to guarantee that the Content-Length value of input messages is never larger than `2147483647`.	https://github.com/OpenSIPS/opensips/commit/7cab422e2fc648f910abba34f3f0dbb3ae171ff5, https://opensips.org/pub/audit-2022/opensips-audit-technical-report-full.pdf	A-OPE-OPEN-280323/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28097		
N/A	15-Mar-2023	7.5	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Prior to versions 3.1.9 and 3.2.6, if `ds_is_in_list()` is used with an invalid IP address string (`NULL` is illegal input), OpenSIPS will attempt to print a string from a random address (stack garbage), which could lead to a crash. All users of `ds_is_in_list()` without the `$si` variable as 1st parameter could be affected by this vulnerability to a larger, lesser or no extent at all, depending if the data passed to the function is a valid IPv4 or IPv6 address string or not. Fixes will are available starting with the 3.1.9 and 3.2.6 minor releases. There are no known workarounds. **CVE ID : CVE-2023-28099**	https://github.com/OpenSIPS/opensips/commit/e2f13d374	A-OPE-OPEN-280323/583
Vendor: openzeppelin					
Product: contracts					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.8.0 Up to (excluding) 4.8.2					
Incorrect Calculation	03-Mar-2023	6.5	OpenZeppelin Contracts is a library for secure smart contract development. The ERC721Consecutive contract designed for minting NFTs in batches does not update balances when a batch has size 1 and consists of a single token. Subsequent transfers from the receiver of that token may overflow the balance as reported by `balanceOf`. The issue exclusively presents with batches of size 1. The issue has been patched in 4.8.2. **CVE ID : CVE-2023-26488**	https://github.com/OpenZeppelin/openzeppelin-contracts/commit/167bf67ed3907f4a674043496019fa346cee7705	A-OPE-CONT-280323/584
Product: contracts_upgradeable					
Affected Version(s): From (including) 4.8.0 Up to (excluding) 4.8.2					
Incorrect Calculation	03-Mar-2023	6.5	OpenZeppelin Contracts is a library for secure smart contract development. The ERC721Consecutive contract designed for minting NFTs in batches does not update balances when a batch has size 1 and consists of a single token.	https://github.com/OpenZeppelin/openzeppelin-contracts/commit/167bf67ed3907f4a674043496019fa346cee7705	A-OPE-CONT-280323/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Subsequent transfers from the receiver of that token may overflow the balance as reported by `balanceOf`. The issue exclusively presents with batches of size 1. The issue has been patched in 4.8.2. **CVE ID : CVE-2023-26488**		
Vendor: optinmonster					
Product: optinmonster					
Affected Version(s): * Up to (excluding) 2.12.2					
N/A	13-Mar-2023	6.5	The Popup Builder by OptinMonster WordPress plugin before 2.12.2 does not ensure that the campaign to be loaded via some shortcodes is actually a campaign, allowing any authenticated users such as subscriber to retrieve the content of arbitrary posts, like draft, private or even password protected ones. **CVE ID : CVE-2023-0772**	N/A	A-OPT-OPTI-280323/586
Vendor: osgeo					
Product: owslib					
Affected Version(s): * Up to (excluding) 0.28.1					
Improper Restriction of XML	08-Mar-2023	7.5	OWSLib is a Python package for client programming with	https://github.com/geopython/OWSLi	A-OSG-OWSL-280323/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			Open Geospatial Consortium (OGC) web service interface standards, and their related content models. OWSLib's XML parser (which supports both `lxml` and `xml.etree`) does not disable entity resolution, and could lead to arbitrary file reads from an attacker-controlled XML payload. This affects all XML parsing in the codebase. This issue has been addressed in version 0.28.1. All users are advised to upgrade. The only known workaround is to patch the library manually. See `GHSA-8h9c-r582-mggc` for details. **CVE ID : CVE-2023-27476**	b/security/advisories/GHSA-8h9c-r582-mggc, https://github.com/geopython/OWSLib/pull/863/commits/b92687702be9576c0681bb11cad21eb631b9122f	
Vendor: panindex_project					
Product: panindex					
Affected Version(s): * Up to (excluding) 3.1.3					
Use of Hard-coded Credentials	13-Mar-2023	9.8	PanIndex is a network disk directory index. In Panindex prior to version 3.1.3, a hard-coded JWT key `PanIndex` is used. An attacker can use the hard-coded JWT key to sign JWT	https://github.com/px-org/PanIndex/security/advisories/GHSA-82wq-gmw8-g87v, https://github.com/px-org/PanInde	A-PAN-PANI-280323/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			token and perform any actions as a user with admin privileges. Version 3.1.3 has a patch for the issue. As a workaround, one may change the JWT key in the source code before compiling the project. **CVE ID : CVE-2023-27583**	x/commit/f7ec0c5739af055ad3a825a20294a5c01ada3302	
Vendor: perfree					
Product: perfreeblog					
Affected Version(s): 3.1.1					
Unrestricted Upload of File with Dangerous Type	15-Mar-2023	9.8	An arbitrary file upload vulnerability in the /admin/user/uploadImg component of PerfreeBlog v3.1.1 allows attackers to execute arbitrary code via a crafted JPG file. **CVE ID : CVE-2023-27757**	N/A	A-PER-PERF-280323/589
Vendor: phone_shop_sales_managements_system_project					
Product: phone_shop_sales_managements_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	08-Mar-2023	6.1	A vulnerability classified as problematic was found in SourceCodester Phone Shop Sales Managements System 1.0. This vulnerability affects	N/A	A-PHO-PHON-280323/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			unknown code of the file /osms/assets/plugins/jquery-validation-1.11.1/demo/captcha/index.php of the component CAPTCHA Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222598 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1275**		
Vendor: PHP					
Product: php					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.0.28					
Use of Password Hash With Insufficient Computational Effort	01-Mar-2023	6.2	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, password_verify() function may accept some invalid Blowfish hashes as valid. If such invalid hash ever ends up in the password database, it may lead to an application allowing any password for this entry as valid. **CVE ID : CVE-2023-0567**	https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4, https://bugs.php.net/bug.php?id=81744	A-PHP-PHP-280323/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.16					
Use of Password Hash With Insufficient Computational Effort	01-Mar-2023	6.2	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, password_verify() function may accept some invalid Blowfish hashes as valid. If such invalid hash ever ends up in the password database, it may lead to an application allowing any password for this entry as valid. **CVE ID : CVE-2023-0567**	https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4, https://bugs.php.net/bug.php?id=81744	A-PHP-PHP-280323/592
Affected Version(s): From (including) 8.2.0 Up to (excluding) 8.2.3					
Use of Password Hash With Insufficient Computational Effort	01-Mar-2023	6.2	In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, password_verify() function may accept some invalid Blowfish hashes as valid. If such invalid hash ever ends up in the password database, it may lead to an application allowing any password for this entry as valid. **CVE ID : CVE-2023-0567**	https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4, https://bugs.php.net/bug.php?id=81744	A-PHP-PHP-280323/593
Vendor: Phpipam					
Product: phpipam					
Affected Version(s): * Up to (excluding) 1.5.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Mar-2023	7.2	SQL Injection in GitHub repository phpipam/phpipam prior to v1.5.2. **CVE ID : CVE-2023-1211**	https://github.com/phpipam/phpipam/commit/16e7a94fb69412e569ccf6f2fe0a1f847309c922, https://hunt r.dev/bounties/ed569124-2aeb-4b0d-a312-435460892afd	A-PHP-PHPI-280323/594
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository phpipam/phpipam prior to v1.5.2. **CVE ID : CVE-2023-1212**	https://hunt r.dev/bounties/3d5199d6-9bb2-4f7b-bd81-bded704da499, https://github.com/phpipam/phpipam/commit/78e0470100a6cb143fe9af2e336dce80e4620960	A-PHP-PHPI-280323/595
Affected Version(s): 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	6.1	phpipam v1.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the closeClass parameter at /subnet-masks/popup.php. **CVE ID : CVE-2023-24657**	https://github.com/phpipam/phpipam/issues/3738	A-PHP-PHPI-280323/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: phpseclib					
Product: phpseclib					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.19					
Loop with Unreachable Exit Condition ('Infinite Loop')	03-Mar-2023	7.5	Math/PrimeField.php in phpseclib 3.x before 3.0.19 has an infinite loop with composite primefields. **CVE ID : CVE-2023-27560**	https://github.com/phpseclib/phpseclib/commit/6298d1cd55c3ffa44533bd41906caec246b60440, https://github.com/phpseclib/phpseclib/releases/tag/3.0.19	A-PHP-PHPS-280323/597
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18. **CVE ID : CVE-2023-1115**	https://huntr.dev/bounties/cfa80332-e4cf-4d64-b3e5-e10298628d17, https://github.com/pimcore/pimcore/commit/c6368b7cc69a3ebf2c83de7586f492ca1f404dd3	A-PIM-PIMC-280323/598
Improper Neutralization of Input During Web Page Generation	01-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18. **CVE ID : CVE-2023-1116**	https://github.com/pimcore/pimcore/commit/f6d322efa207a737eedd8726b7c92e957a	A-PIM-PIMC-280323/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				83341e, https://hunt r.dev/bounti es/3245ff99-9adf-4db9-af94-f995747e09d1	
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.18. **CVE ID : CVE-2023-1117**	https://gith ub.com/pimc ore/pimcore /commit/b9 ba69f66d6a 9986fb36f23 9661b98cd3 3a89853, https://hunt r.dev/bounti es/e8c0044d -a31b-4347-b2d5-59fbf492da3 9	A-PIM-PIMC-280323/600
Affected Version(s): * Up to (excluding) 10.5.19					
Improper Neutralizat ion of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.19. **CVE ID : CVE-2023-1286**	https://hunt r.dev/bounti es/31d9744 2-3f87-439f-83f0-1c7862ef0c7 c, https://gith ub.com/pimc ore/pimcore /commit/82 cca7f4a7560 b160336cce 2610481098 ca52c18	A-PIM-PIMC-280323/601
Improper Neutralizat ion of Input	10-Mar-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository	https://hunt r.dev/bounti es/2a64a32 d-b1cc-4def-	A-PIM-PIMC-280323/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			pimcore/pimcore prior to 10.5.19. **CVE ID : CVE-2023-1312**	91da-18040d59f356, https://github.com/pimcore/pimcore/commit/d35d0712858f24d0ec96ddfd4cbe82ff4b5a5fbb	
Affected Version(s): * Up to (excluding) 11.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2023	5.4	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 11.0.0. **CVE ID : CVE-2023-1247**	https://github.com/pimcore/pimcore/commit/da2af2d413b144b9a742118124457d13232d31fd, https://hunt r.dev/bounties/04447124-c7d4-477f-8364-91fe5b59cda0	A-PIM-PIMC-280323/603
Vendor: pixelyoursite					
Product: pixelyoursite					
Affected Version(s): * Up to (excluding) 9.3.1					
Cross-Site Request Forgery (CSRF)	13-Mar-2023	4.3	Cross-Site Request Forgery (CSRF) vulnerability in PixelYourSite PixelYourSite – Your smart PIXEL (TAG) Manager plugin <= 9.3.0 versions. **CVE ID : CVE-2023-22700**	N/A	A-PIX-PIXE-280323/604
Vendor: plainware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: locatoraid					
Affected Version(s): * Up to (including) 3.9.11					
Cross-Site Request Forgery (CSRF)	15-Mar-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Plainware Locatoraid Store Locator plugin <= 3.9.11 versions. **CVE ID : CVE-2023-25709**	N/A	A-PLA-LOCA-280323/605
Vendor: pmb_project					
Product: pmb					
Affected Version(s): 7.4.6					
Use After Free	06-Mar-2023	9.8	An arbitrary file upload vulnerability in the camera_upload.php component of PMB v7.4.6 allows attackers to execute arbitrary code via a crafted image file. **CVE ID : CVE-2023-24734**	N/A	A-PMB-PMB-280323/606
N/A	06-Mar-2023	9.8	PMB v7.4.6 was discovered to contain a remote code execution (RCE) vulnerability via the component /sauvegarde/restaure_act.php. **CVE ID : CVE-2023-24736**	N/A	A-PMB-PMB-280323/607
Improper Neutralization of Input During	06-Mar-2023	6.1	PMB v7.4.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability	N/A	A-PMB-PMB-280323/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			via the query parameter at /admin/convert/export_z3950_new.php. **CVE ID : CVE-2023-24733**		
URL Redirection to Untrusted Site ('Open Redirect')	06-Mar-2023	6.1	PMB v7.4.6 was discovered to contain an open redirect vulnerability via the component /opac_css/pmb.php. This vulnerability allows attackers to redirect victim users to an external domain via a crafted URL. **CVE ID : CVE-2023-24735**	N/A	A-PMB-PMB-280323/609
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	6.1	PMB v7.4.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the query parameter at /admin/convert/export_z3950.php. **CVE ID : CVE-2023-24737**	N/A	A-PMB-PMB-280323/610
Vendor: Prestashop					
Product: advanced_reviews					
Affected Version(s): * Up to (excluding) 3.6.2					
Improper Neutralization of Special Elements used in an SQL	14-Mar-2023	8.8	PrestaShop ws_productreviews < 3.6.2 is vulnerable to SQL Injection. **CVE ID : CVE-2023-25206**	N/A	A-PRE-ADVA-280323/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')					
Product: dpd_france					
Affected Version(s): * Up to (excluding) 6.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	9.8	PrestaShop dpdfrance <6.1.3 is vulnerable to SQL Injection via dpdfrance/ajax.php. **CVE ID : CVE-2023-25207**	N/A	A-PRE-DPD_-280323/612
Product: xen_forum					
Affected Version(s): * Up to (excluding) 2.13.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Mar-2023	8.8	In the module "Xen Forum" (xenforum) for PrestaShop, an authenticated user can perform SQL injection in versions up to 2.13.0. **CVE ID : CVE-2023-24763**	https://friends-of-presta.github.io/security-advisories/modules/2023/03/06/xenforum.html	A-PRE-XEN_-280323/613
Vendor: prismlauncher					
Product: prism_launcher					
Affected Version(s): * Up to (including) 6.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Mar-2023	7.8	Prism Launcher <= 6.1 is vulnerable to Directory Traversal. **CVE ID : CVE-2023-25304**	https://github.com/PrismLauncher/PrismLauncher/security/advisories/GHSA-wxgx-8v36-mj2m	A-PRI-PRIS-280323/614
Vendor: product_gtin_\(ean\,_upc\,_isbn\)_for_woocommerce_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: product_gtin_\(ean\,_upc\,_isbn\)_for_woocommerce					
Affected Version(s): * Up to (including) 1.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The Product GTIN (EAN, UPC, ISBN) for WooCommerce WordPress plugin through 1.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0068**	N/A	A-PRO-PROD-280323/615
Vendor: Proofpoint					
Product: enterprise_protection					
Affected Version(s): * Up to (excluding) 8.13.22					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	9.8	The webservices in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows for an anonymous user to execute remote code through 'eval injection'. Exploitation requires network access to the webservices API, but such access is a non-standard configuration. This	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0090**		
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	8.8	The webutils in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows an authenticated user to execute remote code through 'eval injection'. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0089**	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/617
Affected Version(s): 8.18.6					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	9.8	The webservices in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows for an anonymous user to execute remote code through 'eval injection'. Exploitation requires network access to the webservices API, but such access is a non-standard configuration. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0090**	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	8.8	The webutils in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows an authenticated user to execute remote code through 'eval injection'. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0089**	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/619
Affected Version(s): 8.20.0					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	9.8	The webservices in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows for an anonymous user to execute remote code through 'eval injection'. Exploitation requires network access to the webservices API, but such access is a non-standard configuration. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0090**	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/620
Improper Control of Generation of Code	08-Mar-2023	8.8	The webutils in Proofpoint Enterprise Protection (PPS/POD) contain a	https://www.proofpoint.com/security/security-advisories/p	A-PRO-ENTE-280323/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			vulnerability that allows an authenticated user to execute remote code through 'eval injection'. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0089**	fpt-sa-2023-0001	
Affected Version(s): From (including) 8.18.0 Up to (excluding) 8.18.4					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	9.8	The webservices in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows for an anonymous user to execute remote code through 'eval injection'. Exploitation requires network access to the webservices API, but such access is a non-standard configuration. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0090**	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/622
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	8.8	The webutils in Proofpoint Enterprise Protection (PPS/POD) contain a vulnerability that allows an authenticated user to execute remote code through 'eval	https://www.proofpoint.com/security/security-advisories/pfpt-sa-2023-0001	A-PRO-ENTE-280323/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection'. This affects all versions 8.20.0 and below. **CVE ID : CVE-2023-0089**		
Vendor: propius					
Product: machineselector					
Affected Version(s): 6.6.0					
Use of Hard-coded Credentials	14-Mar-2023	9.8	A Hard Coded Admin Credentials issue in the Web-UI Admin Panel in Propius MachineSelector 6.6.0 and 6.6.1 allows remote attackers to gain access to the admin panel Propiusadmin.php, which allows taking control of the affected system. **CVE ID : CVE-2023-26511**	https://www.propius.de/ms_security.html	A-PRO-MACH-280323/624
Affected Version(s): 6.6.1					
Use of Hard-coded Credentials	14-Mar-2023	9.8	A Hard Coded Admin Credentials issue in the Web-UI Admin Panel in Propius MachineSelector 6.6.0 and 6.6.1 allows remote attackers to gain access to the admin panel Propiusadmin.php, which allows taking control of the affected system. **CVE ID : CVE-2023-26511**	https://www.propius.de/ms_security.html	A-PRO-MACH-280323/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: pttemkart					
Product: pttem_kart					
Affected Version(s): * Up to (excluding) 2.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ulkem Company PtteM Kart.This issue affects PtteM Kart: before 2.1. **CVE ID : CVE-2023-1267**	N/A	A-PTT-PTTE-280323/626
Vendor: Qemu					
Product: qemu					
Affected Version(s): 7.2.0					
Out-of-bounds Write	06-Mar-2023	9.8	A vulnerability in the lsi53c895a device affects the latest version of qemu. A DMA-MMIO reentrancy problem may lead to memory corruption bugs like stack overflow or use-after-free. **CVE ID : CVE-2023-0330**	https://lists.nongnu.org/archive/html/qemu-devel/2023-01/msg03411.html	A-QEM-QEMU-280323/627
Vendor: quickentity_editor_project					
Product: quickentity_editor					
Affected Version(s): * Up to (excluding) 1.28.1					
Improper Neutralization of Input During	06-Mar-2023	6.1	quickentity-editor-next is an open source, system local, video game asset editor. In affected	https://github.com/atampy25/quickentity-editor-next/commit	A-QUI-QUIC-280323/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			versions HTML tags in entity names are not sanitised (XSS vulnerability). Allows arbitrary code execution within the browser sandbox, among other things, simply from loading a file containing a script tag in any entity name. This issue has been patched in version 1.28.1 of the application. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-27472**	/5303b45a20a6e4e9318729b8dd7bbf09b37b369d	
Vendor: rack_project					
Product: rack					
Affected Version(s): * Up to (excluding) 2.0.9.3					
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected. **CVE ID : CVE-2023-27530**	https://discuss.rubyonrails.org/t/cve-2023-27530-possible-dos-vulnerability-in-multipart-mime-parsing/82388	A-RAC-RACK-280323/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.1.0 Up to (excluding) 2.1.4.3					
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected. **CVE ID : CVE-2023-27530**	https://discuss.rubyonrails.org/t/cve-2023-27530-possible-dos-vulnerability-in-multipart-mime-parsing/82388	A-RAC-RACK-280323/630
Affected Version(s): From (including) 2.2.0 Up to (excluding) 2.2.6.3					
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected. **CVE ID : CVE-2023-27530**	https://discuss.rubyonrails.org/t/cve-2023-27530-possible-dos-vulnerability-in-multipart-mime-parsing/82388	A-RAC-RACK-280323/631
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.4.2					
Allocation of Resources Without Limits or Throttling	10-Mar-2023	7.5	A DoS vulnerability exists in Rack <v3.0.4.2, <v2.2.6.3, <v2.1.4.3 and <v2.0.9.3 within in the Multipart MIME parsing code in	https://discuss.rubyonrails.org/t/cve-2023-27530-possible-dos-	A-RAC-RACK-280323/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could allow an attacker to craft requests that can be abuse to cause multipart parsing to take longer than expected. **CVE ID : CVE-2023-27530**	vulnerability-in-multipart-mime-parsing/82388	
Vendor: Radare					
Product: radare2					
Affected Version(s): 5.8.3					
NULL Pointer Dereference	10-Mar-2023	5.5	radare2 v5.8.3 was discovered to contain a segmentation fault via the component wasm_dis at p/wasm/wasm.c. **CVE ID : CVE-2023-27114**	https://github.com/radareorg/radare2/commit/13308c9aad79f9c7a3507ce549fe270103e8ceea	A-RAD-RADA-280323/633
Vendor: rami					
Product: pretix					
Affected Version(s): 4.16.0					
Insufficient Session Expiration	06-Mar-2023	7.5	rami.io pretix before 4.17.1 allows OAuth application authorization from a logged-out session. The fixed versions are 4.15.1, 4.16.1, and 4.17.1. **CVE ID : CVE-2023-27891**	https://pretix.eu/about/en/blog/20230306-release-4171/	A-RAM-PRET-280323/634
Affected Version(s): 4.17.0					
Insufficient Session Expiration	06-Mar-2023	7.5	rami.io pretix before 4.17.1 allows OAuth application authorization from a	https://pretix.eu/about/en/blog/20230306-	A-RAM-PRET-280323/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logged-out session. The fixed versions are 4.15.1, 4.16.1, and 4.17.1. **CVE ID : CVE-2023-27891**	release-4171/	
Affected Version(s): From (including) 1.16.0 Up to (excluding) 4.15.1					
Insufficient Session Expiration	06-Mar-2023	7.5	rami.io pretix before 4.17.1 allows OAuth application authorization from a logged-out session. The fixed versions are 4.15.1, 4.16.1, and 4.17.1. **CVE ID : CVE-2023-27891**	https://pretix.eu/about/en/blog/20230306-release-4171/	A-RAM-PRET-280323/636
Vendor: rangerstudio					
Product: directus					
Affected Version(s): * Up to (excluding) 9.23.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	Directus is a real-time API and App dashboard for managing SQL database content. Instances relying on an allow-listed reset URL are vulnerable to an HTML injection attack through the use of query parameters in the reset URL. An attacker could exploit this to email users urls to the servers domain but which may contain malicious code. The problem has been resolved and	https://github.com/directus/directus/pull/17120, https://github.com/directus/directus/security/advisories/GHSA-4hmq-ggrm-qfc6	A-RAN-DIRE-280323/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			released under version 9.23.0. People relying on a custom password reset URL should upgrade to 9.23.0 or later, or remove the custom reset url from the configured allow list. Users are advised to upgrade. Users unable to upgrade may disable the custom reset URL allow list as a workaround. **CVE ID : CVE-2023-27474**		
Vendor: rapidload					
Product: power-up_for_autoptimize					
Affected Version(s): * Up to (including) 1.7.1					
Missing Authorization	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the clear_page_cache function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to delete the plugin's cache. **CVE ID : CVE-2023-1333**	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Finclude s%2Fmodules%2Funused-css%2FUnus	A-RAP-POWE-280323/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				edCSS_Admin.php	
Missing Authorization	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized cache modification due to a missing capability check on the queue_posts function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to modify the plugin's cache. **CVE ID : CVE-2023-1334**	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	A-RAP-POWE-280323/639
Missing Authorization	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized plugin settings update due to a missing capability check on the ucss_connect function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to connect a	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmod	A-RAP-POWE-280323/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			new license key to the site. **CVE ID : CVE-2023-1335**	ules%2Funused-css%2FUnusedCSS_Admin.php	
Missing Authorization	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check on the ajax_deactivate function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to disable caching. **CVE ID : CVE-2023-1336**	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	A-RAP-POWE-280323/641
Missing Authorization	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check on the clear_uucss_logs function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funus	A-RAP-POWE-280323/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subscriber-level access to delete plugin log files. **CVE ID : CVE-2023-1337**	edcss%2Ftrunk%2Finclu des%2Fmod ules%2Funu sed-css%2FUnus edCSS_Admi n.php	
Missing Authorizati on	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized cache modification due to a missing capability check on the attach_rule function in versions up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to modify cache rules. **CVE ID : CVE-2023-1338**	https://plugi ns.trac.word press.org/ch angeset/287 7726/unuse dcss/trunk/i ncludes/mo dules/unuse d-css/UnusedC SS_Admin.ph p?contextall =1&old=284 7136&old_pa th=%2Funus edcss%2Ftru nk%2Finclu des%2Fmod ules%2Funu sed-css%2FUnus edCSS_Admi n.php	A-RAP-POWE-280323/643
Missing Authorizati on	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to unauthorized settings update due to a missing capability check on the uucss_update_rule function in versions	https://plugi ns.trac.word press.org/ch angeset/287 7726/unuse dcss/trunk/i ncludes/mo dules/unuse d-css/UnusedC SS_Admin.ph p?contextall	A-RAP-POWE-280323/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			up to, and including, 1.7.1. This makes it possible for authenticated attackers with subscriber-level access to update caching rules. **CVE ID : CVE-2023-1339**	=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	
Cross-Site Request Forgery (CSRF)	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the clear_uucss_logs function. This makes it possible for unauthenticated attackers to clear plugin logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1340**	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	A-RAP-POWE-280323/645
Cross-Site Request Forgery (CSRF)	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/i	A-RAP-POWE-280323/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the ajax_deactivate function. This makes it possible for unauthenticated attackers to turn off caching via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1341**	ncludes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	
Cross-Site Request Forgery (CSRF)	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the ucss_connect function. This makes it possible for unauthenticated attackers to connect the site to a new license key via a forged request granted they can trick a site administrator into performing an action	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	A-RAP-POWE-280323/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as clicking on a link. **CVE ID : CVE-2023-1342**		
Cross-Site Request Forgery (CSRF)	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the attach_rule function. This makes it possible for unauthenticated attackers to modify the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1343**	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	A-RAP-POWE-280323/648
Cross-Site Request Forgery (CSRF)	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the uucss_update_rule function. This makes	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=284	A-RAP-POWE-280323/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it possible for unauthenticated attackers to modify the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1344**	7136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	
Cross-Site Request Forgery (CSRF)	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the queue_posts function. This makes it possible for unauthenticated attackers to modify the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1345**	https://plugins.trac.wordpress.org/changeset/2877726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	A-RAP-POWE-280323/650
Cross-Site Request	10-Mar-2023	4.3	The RapidLoad Power-Up for Autoptimize plugin for WordPress is	https://plugins.trac.wordpress.org/changeset/287	A-RAP-POWE-280323/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.1. This is due to missing or incorrect nonce validation on the clear_page_cache function. This makes it possible for unauthenticated attackers to clear the plugin's cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1346**	7726/unusedcss/trunk/includes/modules/unused-css/UnusedCSS_Admin.php?contextall=1&old=2847136&old_path=%2Funusedcss%2Ftrunk%2Fincludes%2Fmodules%2Funused-css%2FUnusedCSS_Admin.php	
Vendor: readtomyshoe_project					
Product: readtomyshoe					
Affected Version(s): * Up to (excluding) 2023-03-13					
Generation of Error Message Containing Sensitive Information	13-Mar-2023	6.5	ReadtoMyShoe, a web app that lets users upload articles and listen to them later, generates an error message containing sensitive information prior to commit 8533b01. If an error occurs when adding an article, the website shows the user an error message. If the error originates from the Google Cloud TTS request, then it will	https://github.com/rozbb/readtomyshoe/commit/8533b01c818939a0fa919c7244d8dbf5daf032af, https://github.com/rozbb/readtomyshoe/security/advisories/GHSA-23g5-r34j-mr8g	A-REA-READ-280323/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include the full URL of the request. The request URL contains the Google Cloud API key. This has been patched in commit 8533b01. Upgrading should be accompanied by deleting the current GCP API key and issuing a new one. There are no known workarounds. **CVE ID : CVE-2023-27587**		
Vendor: Redhat					
Product: openshift_container_platform					
Affected Version(s): 4.0					
Use of Incorrectly -Resolved Name or Reference	03-Mar-2023	7	runc through 1.1.4 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. NOTE: this issue exists because of a CVE-2019-19921 regression. **CVE ID : CVE-2023-27561**	N/A	A-RED-OPEN-280323/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: redis					
Product: redis					
Affected Version(s): * Up to (excluding) 6.0.18					
Integer Overflow or Wraparound	02-Mar-2023	6.5	Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SRANDMEMBER`, `ZRANDMEMBER`, and `HRANDFIELD` commands can trigger an integer overflow, resulting in a runtime assertion and termination of the Redis server process. This problem affects all Redis versions. Patches were released in Redis version(s) 6.0.18, 6.2.11 and 7.0.9. **CVE ID : CVE-2023-25155**	https://github.com/redis/redis/security/advisories/GHSA-x2r7-j9vw-3w83, https://github.com/redis/redis/commit/2a2a582e7cd99ba3b531336b8bd41df2b566e619	A-RED-REDI-280323/654
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.11					
Integer Overflow or Wraparound	02-Mar-2023	6.5	Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SRANDMEMBER`, `ZRANDMEMBER`, and `HRANDFIELD` commands can trigger an integer overflow, resulting in a runtime assertion and termination of	https://github.com/redis/redis/security/advisories/GHSA-x2r7-j9vw-3w83, https://github.com/redis/redis/commit/2a2a582e7cd99ba3b531336b8b	A-RED-REDI-280323/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Redis server process. This problem affects all Redis versions. Patches were released in Redis version(s) 6.0.18, 6.2.11 and 7.0.9. **CVE ID : CVE-2023-25155**	d41df2b566e619	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.9					
Integer Overflow or Wraparound	02-Mar-2023	6.5	Redis is an in-memory database that persists on disk. Authenticated users issuing specially crafted `SRANDMEMBER`, `ZRANDMEMBER`, and `HRANDFIELD` commands can trigger an integer overflow, resulting in a runtime assertion and termination of the Redis server process. This problem affects all Redis versions. Patches were released in Redis version(s) 6.0.18, 6.2.11 and 7.0.9. **CVE ID : CVE-2023-25155**	https://github.com/redis/redis/security/advisories/GHSA-x2r7-j9vw-3w83, https://github.com/redis/redis/commit/2a2a582e7cd99ba3b531336b8bd41df2b566e619	A-RED-REDI-280323/656
Vendor: resumebuilder					
Product: resume_builder					
Affected Version(s): * Up to (including) 3.1.1					
Improper Neutralization of	06-Mar-2023	5.4	The Resume Builder WordPress plugin through 3.1.1 does	N/A	A-RES-RESU-280323/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			not sanitize and escape some parameters related to Resume, which could allow users with a role as low as subscriber to perform Stored XSS attacks against higher privilege users **CVE ID : CVE-2023-0078**		
Vendor: rizin					
Product: rizin					
Affected Version(s): * Up to (including) 0.5.1					
Out-of-bounds Write	14-Mar-2023	7.8	Rizin is a UNIX-like reverse engineering framework and command-line toolset. In version 0.5.1 and prior, converting a GDB registers profile file into a Rizin register profile can result in a stack-based buffer overflow when the `name`, `type`, or `groups` fields have longer values than expected. Users opening untrusted GDB registers files (e.g. with the `drpg` or `arpg` commands) are affected by this flaw. Commit d6196703d89c84467b600ba2692534579dc25ed4 contains a patch for this issue.	https://github.com/rizinorg/rizin/security/advisories/GHSA-rqcp-m8m2-jcqf, https://github.com/rizinorg/rizin/pull/3422, https://github.com/rizinorg/rizin/commit/d6196703d89c84467b600ba2692534579dc25ed4	A-RIZ-RIZI-280323/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			As a workaround, review the GDB register profiles before loading them with `drpg`/`arpg` commands. **CVE ID : CVE-2023-27590**		
Vendor: rocket.chat					
Product: rocket.chat					
Affected Version(s): * Up to (excluding) 6.0.0					
Inadequate Encryption Strength	10-Mar-2023	7.5	An improper access control vulnerability exists prior to v6 that could allow an attacker to break the E2E encryption of a chat room by a user changing the group key of a chat room. **CVE ID : CVE-2023-23911**	N/A	A-ROC-ROCK-280323/659
Vendor: roxy-wi					
Product: roxy-wi					
Affected Version(s): * Up to (excluding) 6.3.5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-Mar-2023	7.5	Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.5.0 have a directory traversal vulnerability that allows the inclusion of server-side files. This issue is fixed in version 6.3.5.0. **CVE ID : CVE-2023-25803**	https://github.com/hap-wi/roxy-wi/security/advisories/GHSA-cv9w-j9gh-5j3w	A-ROX-ROXY-280323/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Mar-2023	5.3	Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.5.0 have a limited path traversal vulnerability. An SSH key can be saved into an unintended location, for example the `/tmp` folder using a payload `../../../../../tmp/test111_dev`. This issue has been fixed in version 6.3.5.0. **CVE ID : CVE-2023-25804**	N/A	A-ROX-ROXY-280323/661
Affected Version(s): * Up to (excluding) 6.3.6.0					
Exposure of Resource to Wrong Sphere	13-Mar-2023	7.5	Roxy-WI is a Web interface for managing Haproxy, Nginx, Apache, and Keepalived servers. Versions prior to 6.3.6.0 don't correctly neutralize `dir/../filename` sequences, such as `/etc/nginx/../passwd`, allowing an actor to gain information about a server. Version 6.3.6.0 has a patch for this issue. **CVE ID : CVE-2023-25802**	https://github.com/hap-wi/roxy-wi/commit/0054f25da7cf8c7480452f48e39308b5e392dc67, https://github.com/hap-wi/roxy-wi/security/advisories/GHSA-qcmp-q5h3-784m	A-ROX-ROXY-280323/662
Vendor: rsshub					
Product: rsshub					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2023-03-02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	RSSHub is an open source and extensible RSS feed generator. When the URL parameters contain certain special characters, it returns an error page that does not properly handle XSS vulnerabilities, allowing for the execution of arbitrary JavaScript code. Users who access the deliberately constructed URL are affected. This vulnerability was fixed in version c910c4d28717fb860fbe064736641f379fab2c91. Please upgrade to this or a later version, there are no known workarounds. **CVE ID : CVE-2023-26491**	https://github.com/DIYgod/RSSHub/commit/c910c4d28717fb860fbe064736641f379fab2c91, https://github.com/DIYgod/RSSHub/security/advisories/GHSA-32gr-4cq6-5w5q	A-RSS-RSSH-280323/663
Vendor: s-mall-ssm_project					
Product: s-mall-ssm					
Affected Version(s): * Up to (excluding) 2020-02-17					
Improper Neutralization of Input During Web Page Generation	15-Mar-2023	4.8	Cross site scripting (XSS) vulnerability in xenv S-mall-ssm thru commit 3d9e77f7d80289a30f67aaba1ae73e375d33ef71 on Feb 17, 2020, allows local	https://github.com/xenv/S-mall-ssm/issues/37	A-S-M-S-MA-280323/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attackers to execute arbitrary code via the evaluate button. **CVE ID : CVE-2023-26912**		
Vendor: saas.group					
Product: juicer					
Affected Version(s): * Up to (excluding) 1.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Mar-2023	5.4	The Juicer WordPress plugin before 1.11 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-0172**	N/A	A-SAA-JUIC-280323/665
Vendor: saleor					
Product: saleor					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 3.1.48					
Generation of Error Message Containing Sensitive Information	02-Mar-2023	5.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages.	https://github.com/saleor/saleor/security/advisories/GHSA-3hvj-3cg9-v242	A-SAL-SALE-280323/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12. **CVE ID : CVE-2023-26052**		
Generation of Error Message Containing Sensitive Information	02-Mar-2023	4.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like user email address in staff-authenticated requests. **CVE ID : CVE-2023-26051**	https://github.com/saleor/saleor/commit/31bce881ccccf0d79a9b14ecb6ca3138d1edeec1, https://github.com/saleor/saleor/security/advisories/GHSA-r8qr-wwg3-2r85	A-SAL-SALE-280323/667
Affected Version(s): From (including) 3.10.0 Up to (excluding) 3.10.14					
Generation of Error Message Containing Sensitive Information	02-Mar-2023	5.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python	https://github.com/saleor/saleor/security/advisories/GHSA-3hvj-3cg9-v242	A-SAL-SALE-280323/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12. **CVE ID : CVE-2023-26052**		
Generation of Error Message Containing Sensitive Information	02-Mar-2023	4.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like user email address in staff-authenticated requests. **CVE ID : CVE-2023-26051**	https://github.com/saleor/saleor/commit/31bce881ccccf0d79a9b14ecb6ca3138d1edeec1, https://github.com/saleor/saleor/security/advisories/GHSA-r8qr-wwg3-2r85	A-SAL-SALE-280323/669
Affected Version(s): From (including) 3.11.0 Up to (excluding) 3.11.12					
Generation of Error	02-Mar-2023	5.3	Saleor is a headless, GraphQL commerce	https://github.com/saleor	A-SAL-SALE-280323/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Message Containing Sensitive Information			platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12. **CVE ID : CVE-2023-26052**	/saleor/security/advisories/GHSA-3hvj-3cg9-v242	
Generation of Error Message Containing Sensitive Information	02-Mar-2023	4.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like user email address in staff-authenticated requests.	https://github.com/saleor/saleor/commit/31bce881ccccf0d79a9b14ecb6ca3138d1edeec1, https://github.com/saleor/saleor/security/advisories/GHSA-r8qr-wwg3-2r85	A-SAL-SALE-280323/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26051		
Affected Version(s): From (including) 3.2.0 Up to (excluding) 3.7.59					
Generation of Error Message Containing Sensitive Information	02-Mar-2023	5.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12. **CVE ID : CVE-2023-26052**	https://github.com/saleor/saleor/security/advisories/GHSA-3hvj-3cg9-v242	A-SAL-SALE-280323/672
Generation of Error Message Containing Sensitive Information	02-Mar-2023	4.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information	https://github.com/saleor/saleor/commit/31bce881ccccf0d79a9b14ecb6ca3138d1edeec1, https://github.com/saleor/saleor/security/advisories/GHSA-	A-SAL-SALE-280323/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			like user email address in staff-authenticated requests. **CVE ID : CVE-2023-26051**	r8qr-wwg3-2r85	
Affected Version(s): From (including) 3.8.0 Up to (excluding) 3.8.30					
Generation of Error Message Containing Sensitive Information	02-Mar-2023	5.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12. **CVE ID : CVE-2023-26052**	https://github.com/saleor/saleor/security/advisories/GHSA-3hvj-3cg9-v242	A-SAL-SALE-280323/674
Generation of Error Message Containing Sensitive Information	02-Mar-2023	4.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are	https://github.com/saleor/saleor/commit/31bce881ccccf0d79a9b14ecb6ca3138d1edeec1, https://github.com/saleor	A-SAL-SALE-280323/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			returned in API as error messages. Some messages might contain sensitive information like user email address in staff-authenticated requests. **CVE ID : CVE-2023-26051**	/saleor/security/advisories/GHSA-r8qr-wwg3-2r85	
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.27					
Generation of Error Message Containing Sensitive Information	02-Mar-2023	5.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like infrastructure details in unauthenticated requests. This issue has been patched in versions 3.1.48, 3.7.59, 3.8.0, 3.9.27, 3.10.14 and 3.11.12. **CVE ID : CVE-2023-26052**	https://github.com/saleor/saleor/security/advisories/GHSA-3hvj-3cg9-v242	A-SAL-SALE-280323/676
Generation of Error Message Containing Sensitive	02-Mar-2023	4.3	Saleor is a headless, GraphQL commerce platform delivering personalized shopping	https://github.com/saleor/saleor/commit/31bce881ccccf0d79a	A-SAL-SALE-280323/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			experiences. Some internal Python exceptions are not handled properly and thus are returned in API as error messages. Some messages might contain sensitive information like user email address in staff-authenticated requests. **CVE ID : CVE-2023-26051**	9b14ecb6ca3138d1edeec1, https://github.com/saleor/saleor/security/advisories/GHSA-r8qr-wwg3-2r85	
Vendor: sales_tracker_management_system_project					
Product: sales_tracker_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Sales Tracker Management System 1.0. Affected by this issue is some unknown functionality of the file admin/clients/view_client.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier	https://github.com/Mart1nD0t/vul-test/blob/main/sts-1.md	A-SAL-SALE-280323/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-222644. **CVE ID : CVE-2023-1290**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/clients/manage_client.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222645 was assigned to this vulnerability. **CVE ID : CVE-2023-1291**	https://github.com/Mart1nD0t/vul-test/blob/main/sts-2.md	A-SAL-SALE-280323/679
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Mar-2023	9.8	A vulnerability has been found in SourceCodester Sales Tracker Management System 1.0 and classified as critical. This vulnerability affects the function delete_client of the file classes/Master.php. The manipulation of the argument id leads to sql injection.	https://github.com/Mart1nD0t/vul-test/blob/main/sts-3.md	A-SAL-SALE-280323/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222646 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1292**		
Vendor: SAP					
Product: abap_platform					
Affected Version(s): 751					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	4.9	Due to insufficient input sanitization, SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and integrity of the application. **CVE ID : CVE-2023-25615**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-280323/681
Affected Version(s): 753					
Improper Neutralizat	14-Mar-2023	4.9	Due to insufficient input sanitization,	https://www.sap.com/d	A-SAP-ABAP-280323/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and integrity of the application. **CVE ID : CVE-2023-25615**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 754					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	4.9	Due to insufficient input sanitization, SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-280323/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity of the application. **CVE ID : CVE-2023-25615**		
Affected Version(s): 756					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	4.9	Due to insufficient input sanitization, SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and integrity of the application. **CVE ID : CVE-2023-25615**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-280323/684
Affected Version(s): 757					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	4.9	Due to insufficient input sanitization, SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-280323/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and integrity of the application. **CVE ID : CVE-2023-25615**		
Affected Version(s): 791					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	4.9	Due to insufficient input sanitization, SAP ABAP - versions 751, 753, 753, 754, 756, 757, 791, allows an authenticated high privileged user to alter the current session of the user by injecting the malicious database queries over the network and gain access to the unintended data. This may lead to a high impact on the confidentiality and no impact on the availability and integrity of the application. **CVE ID : CVE-2023-25615**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-280323/686
Product: authenticator					
Affected Version(s): 1.3.0					
Privilege Defined With	14-Mar-2023	6.5	SAP Authenticator for Android - version 1.3.0, allows the	https://www.sap.com/documents/2	A-SAP-AUTH-280323/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unsafe Actions			screen to be captured, if an authorized attacker installs a malicious app on the mobile device. The attacker could extract the currently views of the OTP and the secret OTP alphanumeric token during the token setup. On successful exploitation, an attacker can read some sensitive information but cannot modify and delete the data. **CVE ID : CVE-2023-27895**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Product: businessobjects_business_intelligence					
Affected Version(s): 420					
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.5	In SAP BusinessObjects Business Intelligence Platform - version 420, 430, an attacker can control a malicious BOE server, forcing the application server to connect to its own CMS, leading to a high impact on availability. **CVE ID : CVE-2023-27896**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/688
Exposure of Sensitive Information to an	14-Mar-2023	5.3	SAP BusinessObjects Business Intelligence Platform (Web Services) - versions	https://www.sap.com/documents/2022/02/fa86	A-SAP-BUSI-280323/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			420, 430, allows an attacker to inject arbitrary values as CMS parameters to perform lookups on the internal network which is otherwise not accessible externally. On successful exploitation, attacker can scan internal network to determine internal infrastructure for further attacks like remote file inclusion, retrieve server files, bypass firewall and force the vulnerable server to execute malicious requests, resulting in sensitive information disclosure. This causes limited impact on confidentiality of data. **CVE ID : CVE-2023-27894**	5ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 430					
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.5	In SAP BusinessObjects Business Intelligence Platform - version 420, 430, an attacker can control a malicious BOE server, forcing the application server to connect to its own CMS, leading to a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high impact on availability. **CVE ID : CVE-2023-27896**		
Exposure of Sensitive Information to an Unauthorized Actor	14-Mar-2023	5.3	SAP BusinessObjects Business Intelligence Platform (Web Services) - versions 420, 430, allows an attacker to inject arbitrary values as CMS parameters to perform lookups on the internal network which is otherwise not accessible externally. On successful exploitation, attacker can scan internal network to determine internal infrastructure for further attacks like remote file inclusion, retrieve server files, bypass firewall and force the vulnerable server to execute malicious requests, resulting in sensitive information disclosure. This causes limited impact on confidentiality of data. **CVE ID : CVE-2023-27894**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/691
Product: businessobjects_business_intelligence_platform					
Affected Version(s): 420					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.5	In SAP BusinessObjects Business Intelligence Platform (Web Services) - versions 420, 430, an attacker can control a malicious BOE server, forcing the application server to connect to its own admintools, leading to a high impact on availability. **CVE ID : CVE-2023-27271**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/692
Affected Version(s): 430					
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.5	In SAP BusinessObjects Business Intelligence Platform (Web Services) - versions 420, 430, an attacker can control a malicious BOE server, forcing the application server to connect to its own admintools, leading to a high impact on availability. **CVE ID : CVE-2023-27271**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/693
Product: business_objects_business_intelligence_platform					
Affected Version(s): 420					
Improper Neutralization of Special Elements in Output Used by a	14-Mar-2023	8.8	In some scenario, SAP Business Objects Business Intelligence Platform (CMC) - versions 420, 430, Program Object execution can lead to	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-BUSI-280323/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			code injection vulnerability which could allow an attacker to gain access to resources that are allowed by extra privileges. Successful attack could highly impact the confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2023-25616**	c68f7e60039b.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Mar-2023	8.8	SAP Business Object (Adaptive Job Server) - versions 420, 430, allows remote execution of arbitrary commands on Unix, when program objects execution is enabled, to authenticated users with scheduling rights, using the BI Launchpad, Central Management Console or a custom application based on the public java SDK. Programs could impact the confidentiality, integrity and availability of the system. **CVE ID : CVE-2023-25617**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/695
Affected Version(s): 430					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	14-Mar-2023	8.8	In some scenario, SAP Business Objects Business Intelligence Platform (CMC) - versions 420, 430, Program Object execution can lead to code injection vulnerability which could allow an attacker to gain access to resources that are allowed by extra privileges. Successful attack could highly impact the confidentiality, Integrity, and Availability of the system. **CVE ID : CVE-2023-25616**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/696
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Mar-2023	8.8	SAP Business Object (Adaptive Job Server) - versions 420, 430, allows remote execution of arbitrary commands on Unix, when program objects execution is enabled, to authenticated users with scheduling rights, using the BI Launchpad, Central Management Console or a custom application based on the public java SDK. Programs could impact the confidentiality,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-280323/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity and availability of the system. **CVE ID : CVE-2023-25617**		
Product: content_server					
Affected Version(s): 7.53					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	SAP Content Server - version 7.53, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-26457**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CONT-280323/698
Product: host_agent					
Affected Version(s): 7.22					
Stack-based Buffer Overflow	14-Mar-2023	7.2	SAP Host Agent (SAPOSCOL) - version 7.22, allows an unauthenticated attacker with network access to a server port assigned to the SAP Start Service to submit a crafted request which results in a memory corruption error. This error can be used to reveal but not modify any	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HOST-280323/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			technical information about the server. It can also make a particular service temporarily unavailable **CVE ID : CVE-2023-27498**		
Product: netweaver					
Affected Version(s): 700					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701, 702, 731, 740, 750, allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application. **CVE ID : CVE-2023-0021**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/700
Affected Version(s): 701					
Improper Neutralization of Input During	14-Mar-2023	6.1	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701,	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-280323/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			702, 731, 740, 750, allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application. **CVE ID : CVE-2023-0021**	0010-bca6-c68f7e60039b.html	
Affected Version(s): 702					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701, 702, 731, 740, 750, allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			partially impact confidentiality of the application. **CVE ID : CVE-2023-0021**		
Affected Version(s): 731					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701, 702, 731, 740, 750, allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application. **CVE ID : CVE-2023-0021**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/703
Affected Version(s): 740					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701, 702, 731, 740, 750, allows an unauthenticated attacker to inject	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application. **CVE ID : CVE-2023-0021**		
Affected Version(s): 750					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	Due to insufficient encoding of user input, SAP NetWeaver - versions 700, 701, 702, 731, 740, 750, allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password, which could lead to reflected Cross-Site scripting. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0021		
Product: netweaver_application_server_abap					
Affected Version(s): 751					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/706
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/708
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**		
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/710

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/711
Affected Version(s): 753					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/713
Improper Limitation of a Pathname to a	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-280323/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	0010-bca6-c68f7e60039b.html	
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/715
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731,	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-280323/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	0010-bca6-c68f7e60039b.html	
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**		
Affected Version(s): 754					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/718
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/720
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**		
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25618		
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/723
Affected Version(s): 756					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/725
Improper Limitation of a	14-Mar-2023	8.1	An attacker with non-administrative authorizations can	https://www.sap.com/documents/2	A-SAP-NETW-280323/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/727
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP	https://www.sap.com/documents/2	A-SAP-NETW-280323/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**		
Affected Version(s): 757					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/730
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/732
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-280323/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	c68f7e60039b.html	
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or modify any information. **CVE ID : CVE-2023-25618**		
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/735
Affected Version(s): 791					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/737

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/738
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**		
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/740
Affected Version(s): 700					
Improper Limitation of a	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP	https://www.sap.com/documents/2	A-SAP-NETW-280323/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/743
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**		
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/745
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**		
Affected Version(s): 701					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27269		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/748
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			making the system unavailable. **CVE ID : CVE-2023-27500**		
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/750
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**		
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 702					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/753
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/755
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**		
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/757
Uncontrolled Resource	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731,	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-280323/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	0010-bca6-c68f7e60039b.html	
Affected Version(s): 731					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			making the system unavailable. **CVE ID : CVE-2023-27269**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/760
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**		
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/762
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**		
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27270		
Affected Version(s): 740					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/765
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/767
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**		
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/769
Uncontrolled Resource	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP	https://www.sap.com/documents/2	A-SAP-NETW-280323/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 750					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/772
Improper Limitation of a Pathname to a Restricted Directory	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-280323/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	c68f7e60039b.html	
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/774
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-280323/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	c68f7e60039b.html	
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or modify any information. **CVE ID : CVE-2023-27270**		
Affected Version(s): 752					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/777
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/779
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**		
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/782
Affected Version(s): 755					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker with non-administrative authorizations to exploit a directory traversal flaw in an available service to overwrite the system	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			files. In this attack, no data can be read but potentially critical OS files can be overwritten making the system unavailable. **CVE ID : CVE-2023-27269**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	9.6	SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker to exploit insufficient validation of path information provided by users, thus exploiting a directory traversal flaw in an available service to delete system files. In this attack, no data can be read but potentially critical OS files can be deleted making the system unavailable, causing significant impact on both availability and integrity **CVE ID : CVE-2023-27501**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/784
Improper Limitation of a Pathname to a	14-Mar-2023	8.1	An attacker with non-administrative authorizations can exploit a directory traversal flaw in	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-280323/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			program SAPRSBRO to over-write system files. In this attack, no data can be read but potentially critical OS files can be over-written making the system unavailable. **CVE ID : CVE-2023-27500**	0010-bca6-c68f7e60039b.html	
Server-Side Request Forgery (SSRF)	14-Mar-2023	7.4	Due to improper input controls In SAP NetWeaver AS for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, an attacker authenticated as a non-administrative user can craft a request which will trigger the application server to send a request to an arbitrary URL which can reveal, modify or make unavailable non-sensitive information, leading to low impact on Confidentiality, Integrity and Availability. **CVE ID : CVE-2023-26459**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/786
N/A	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731,	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-280323/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in an unused class for error handling in which an attacker authenticated as a non-administrative user can craft a request with certain parameters which will consume the server's resources sufficiently to make it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-25618**	0010-bca6-c68f7e60039b.html	
Uncontrolled Resource Consumption	14-Mar-2023	6.5	SAP NetWeaver Application Server for ABAP and ABAP Platform - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, has multiple vulnerabilities in a class for test purposes in which an attacker authenticated as a non-administrative user can craft a request with certain parameters, which will consume the server's resources sufficiently to make	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it unavailable. There is no ability to view or modify any information. **CVE ID : CVE-2023-27270**		
Product: netweaver_application_server_for_java					
Affected Version(s): 7.50					
Improper Authentication	14-Mar-2023	8.6	Due to missing authentication check, SAP NetWeaver AS for Java - version 7.50, allows an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and services across systems. On a successful exploitation, the attacker can read and modify some sensitive information but can also be used to lock up any element or operation of the system making that it unresponsive or unavailable. **CVE ID : CVE-2023-23857**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/789
Improper Access Control	14-Mar-2023	5.3	Cache Management Service in SAP NetWeaver	https://www.sap.com/documents/2	A-SAP-NETW-280323/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Application Server for Java - version 7.50, does not perform any authentication checks for functionalities that require user identity **CVE ID : CVE-2023-26460**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Improper Access Control	14-Mar-2023	5.3	SAP NetWeaver AS Java (Object Analyzing Service) - version 7.50, does not perform necessary authorization checks, allowing an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access a service which will enable them to access but not modify server settings and data with no effect on availability., resulting in escalation of privileges. **CVE ID : CVE-2023-27268**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/791
Product: netweaver_application_server_java					
Affected Version(s): 7.50					
Missing Authentication for	14-Mar-2023	5.3	SAP NetWeaver Application Server Java for Classload Service - version	https://www.sap.com/documents/2022/02/fa86	A-SAP-NETW-280323/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			7.50, does not perform any authentication checks for functionalities that require user identity, resulting in escalation of privileges. This failure has a low impact on confidentiality of the data such that an unassigned user can read non-sensitive server data. **CVE ID : CVE-2023-24526**	5ea4-167e-0010-bca6-c68f7e60039b.html	
Product: netweaver_enterprise_portal					
Affected Version(s): 7.50					
Improper Restriction of XML External Entity Reference	14-Mar-2023	4.9	SAP NetWeaver allows (SAP Enterprise Portal) - version 7.50, allows an authenticated attacker with sufficient privileges to access the XML parser which can submit a crafted XML file which when parsed will enable them to access but not modify sensitive files and data. It allows the attacker to view sensitive data which is owned by certain privileges. **CVE ID : CVE-2023-26461**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-280323/793
Vendor: sauter-controls					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bacnetstac					
Affected Version(s): * Up to (including) 4.2.1					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	A-SAU-BACN-280323/794
Vendor: saysis					
Product: starcities					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saysis Starcities allows SQL Injection.This issue affects Starcities: through 1.3.	N/A	A-SAY-STAR-280323/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1198		
Files or Directories Accessible to External Parties	10-Mar-2023	7.5	Files or Directories Accessible to External Parties vulnerability in Saysis Starcities allows Collect Data from Common Resource Locations.This issue affects Starcities: through 1.3. **CVE ID : CVE-2023-1246**	N/A	A-SAY-STAR-280323/796
Vendor: scriptless_social_sharing_project					
Product: scriptless_social_sharing					
Affected Version(s): * Up to (excluding) 3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The Scriptless Social Sharing WordPress plugin before 3.2.2 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0377**	N/A	A-SCR-SCRI-280323/797
Vendor: shadowsocks					
Product: shadowsocksx-ng					
Affected Version(s): 1.10.0					
N/A	03-Mar-2023	9.8	ShadowsocksX-NG 1.10.0 signs with	https://github.com/shado	A-SHA-SHAD-280323/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			com.apple.security.get-task-allow entitlements because of CODE_SIGNING_INJECT_BASE_ENTITLEMENTS. **CVE ID : CVE-2023-27574**	wsocks/ShadowsocksX-NG/pull/1456	
Vendor: Shopex					
Product: ecshop					
Affected Version(s): * Up to (including) 4.1.8					
Unrestricted Upload of File with Dangerous Type	06-Mar-2023	8.8	A vulnerability, which was classified as problematic, has been found in ECshop up to 4.1.8. Affected by this issue is some unknown functionality of the file admin/database.php of the component Backup Database Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222356. **CVE ID : CVE-2023-1184**	N/A	A-SHO-ECSH-280323/799
Unrestricted Upload of File with	06-Mar-2023	8.8	A vulnerability, which was classified as problematic, was found in ECshop up	N/A	A-SHO-ECSH-280323/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			to 4.1.8. This affects an unknown part of the component New Product Handler. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222357 was assigned to this vulnerability. **CVE ID : CVE-2023-1185**		
Vendor: Siemens					
Product: ruggedcom_crossbow					
Affected Version(s): * Up to (excluding) 5.2					
Missing Authorization	14-Mar-2023	8.8	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.2). The client query handler of the affected application fails to check for proper permissions for specific write queries. This could allow an authenticated remote attacker to perform unauthorized actions. **CVE ID : CVE-2023-27309**	https://cert-portal.siemens.com/productcert/pdf/ssa-260625.pdf	A-SIE-RUGG-280323/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	14-Mar-2023	8.8	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.2). The client query handler of the affected application fails to check for proper permissions when assigning groups to user accounts. This could allow an authenticated remote attacker to assign administrative groups to otherwise non-privileged user accounts. **CVE ID : CVE-2023-27310**	https://cert-portal.siemens.com/productcert/pdf/ssa-260625.pdf	A-SIE-RUGG-280323/802
Affected Version(s): * Up to (excluding) 5.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-Mar-2023	8.8	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.3). The audit log form of affected applications is vulnerable to SQL injection. This could allow authenticated remote attackers to execute arbitrary SQL queries on the server database. **CVE ID : CVE-2023-27463**	https://cert-portal.siemens.com/productcert/pdf/ssa-320629.pdf	A-SIE-RUGG-280323/803
Missing Authorization	14-Mar-2023	4.3	A vulnerability has been identified in RUGGEDCOM	https://cert-portal.siemens.com/prod	A-SIE-RUGG-280323/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CROSSBOW (All versions < V5.3). The client query handler of the affected application fails to check for proper permissions for specific read queries. This could allow authenticated remote attackers to access data they are not authorized for. **CVE ID : CVE-2023-27462**	uctcert/pdf/ssa-320629.pdf	
Product: tecnomatix_plant_simulation					
Affected Version(s): * Up to (excluding) 2201.0006					
Out-of-bounds Write	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20304) **CVE ID : CVE-2023-27398**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-280323/805
Out-of-bounds Write	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TECN-280323/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20299, ZDI-CAN-20346) **CVE ID : CVE-2023-27399**	ssa-847261.pdf	
Out-of-bounds Write	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20300) **CVE ID : CVE-2023-27400**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-280323/807
Out-of-bounds Read	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TECN-280323/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20308, ZDI-CAN-20345) **CVE ID : CVE-2023-27401**	ssa-847261.pdf	
Out-of-bounds Read	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20334) **CVE ID : CVE-2023-27402**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-280323/809
Out-of-bounds Write	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The	https://cert-portal.siemens.com/productcert/pdf/	A-SIE-TECN-280323/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected application contains a memory corruption vulnerability while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20303, ZDI-CAN-20348) **CVE ID : CVE-2023-27403**	ssa-847261.pdf	
Out-of-bounds Write	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to stack-based buffer while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20433) **CVE ID : CVE-2023-27404**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-280323/811
Out-of-bounds Read	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected applications contain an out of bounds read past the	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-280323/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-20432) **CVE ID : CVE-2023-27405**		
Out-of-bounds Write	14-Mar-2023	7.8	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V2201.0006). The affected application is vulnerable to stack-based buffer while parsing specially crafted SPP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-20449) **CVE ID : CVE-2023-27406**	https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf	A-SIE-TECN-280323/813
Vendor: simple_art_gallery_project					
Product: simple_art_gallery					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	15-Mar-2023	9.8	A vulnerability classified as critical has been found in Simple Art Gallery 1.0. Affected is an unknown function of the file adminHome.php.	https://github.com/Songs-YZS/CveList/blob/main/SIMPLE%20ART%20GALLERY%20sys	A-SIM-SIMP-280323/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			The manipulation of the argument social_facebook leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-223128. **CVE ID : CVE-2023-1416**	tem%20has%20Sql%20injection%20vulnerabilities.pdf	
Unrestricted Upload of File with Dangerous Type	15-Mar-2023	8.8	A vulnerability was found in Simple Art Gallery 1.0. It has been declared as critical. This vulnerability affects the function sliderPicSubmit of the file adminHome.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-223126 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1415**	N/A	A-SIM-SIMP-280323/815
Vendor: simple_bakery_shop_management_system_project					
Product: simple_bakery_shop_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	12-Mar-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester	N/A	A-SIM-SIMP-280323/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Simple Bakery Shop Management System 1.0. Affected by this issue is some unknown functionality of the component Admin Login. The manipulation of the argument username/password with the input admin' or 1=1 -- leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222860. **CVE ID : CVE-2023-1357**		
Vendor: simple_customer_relationship_management_system_project					
Product: simple_customer_relationship_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Mar-2023	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the contact parameter in the user profile update function. **CVE ID : CVE-2023-24728**	https://github.com/rahulpatwari/CVE/blob/main/CVE-2023-24728/CVE-2023-24728.txt	A-SIM-SIMP-280323/817
Improper Neutralization of	15-Mar-2023	8.8	Simple Customer Relationship Management System	https://github.com/rahulpatwari/CVE	A-SIM-SIMP-280323/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			v1.0 as discovered to contain a SQL injection vulnerability via the address parameter in the user profile update function. **CVE ID : CVE-2023-24729**	/blob/main/CVE-2023-24729/CVE-2023-24729.txt	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Mar-2023	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the company parameter in the user profile update function. **CVE ID : CVE-2023-24730**	https://github.com/rahulpatwari/CVE/blob/main/CVE-2023-24730/CVE-2023-24730.txt	A-SIM-SIMP-280323/819
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Mar-2023	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the query parameter in the user profile update function. **CVE ID : CVE-2023-24731**	https://github.com/rahulpatwari/CVE/blob/main/CVE-2023-24731/CVE-2023-24731.txt	A-SIM-SIMP-280323/820
Improper Neutralization of Special Elements used in an SQL Command	15-Mar-2023	8.8	Simple Customer Relationship Management System v1.0 as discovered to contain a SQL injection vulnerability via the gender parameter in	https://github.com/rahulpatwari/CVE/blob/main/CVE-2023-24732/CVE-2023-24732.txt	A-SIM-SIMP-280323/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			the user profile update function. **CVE ID : CVE-2023-24732**		
Vendor: simple_payroll_system_with_dynamic_tax_bracket_project					
Product: simple_payroll_system_with_dynamic_tax_bracket					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	4.8	A vulnerability was found in SourceCodester Simple Payroll System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file admin/?page=admin of the component POST Parameter Handler. The manipulation of the argument fullname leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222073 was assigned to this vulnerability. **CVE ID : CVE-2023-1113**	N/A	A-SIM-SIMP-280323/822
Vendor: Sitecore					
Product: experience_manager					
Affected Version(s): 10.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	14-Mar-2023	8.8	An issue was discovered in Sitecore XP/XM 10.3. As an authenticated Sitecore user, a unrestricted language file upload vulnerability exists the can lead to direct code execution on the content management (CM) server. **CVE ID : CVE-2023-26262**	https://www.sitecore.com/trust	A-SIT-EXPE-280323/823
Product: experience_platform					
Affected Version(s): 10.3					
Unrestricted Upload of File with Dangerous Type	14-Mar-2023	8.8	An issue was discovered in Sitecore XP/XM 10.3. As an authenticated Sitecore user, a unrestricted language file upload vulnerability exists the can lead to direct code execution on the content management (CM) server. **CVE ID : CVE-2023-26262**	https://www.sitecore.com/trust	A-SIT-EXPE-280323/824
Vendor: Smartbear					
Product: zephyr_enterprise					
Affected Version(s): * Up to (including) 7.15					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2023	9.8	SmartBear Zephyr Enterprise through 7.15.0 mishandles user-defined input during report generation. This	https://smartbear.com/security/cve/	A-SMA-ZEPH-280323/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to remote code execution by unauthenticated users. **CVE ID : CVE-2023-22889**		
Incorrect Authorization	08-Mar-2023	8.1	There exists a privilege escalation vulnerability in SmartBear Zephyr Enterprise through 7.15.0 that could be exploited by authorized users to reset passwords for other accounts. **CVE ID : CVE-2023-22891**	https://smartbear.com/security/cve/	A-SMA-ZEPH-280323/826
Unrestricted Upload of File with Dangerous Type	08-Mar-2023	7.5	SmartBear Zephyr Enterprise through 7.15.0 allows unauthenticated users to upload large files, which could exhaust the local drive space, causing a denial of service condition. **CVE ID : CVE-2023-22890**	https://smartbear.com/security/cve/	A-SMA-ZEPH-280323/827
Exposure of Resource to Wrong Sphere	08-Mar-2023	7.5	There exists an information disclosure vulnerability in SmartBear Zephyr Enterprise through 7.15.0 that could be exploited by unauthenticated users to read arbitrary files from Zephyr instances.	https://smartbear.com/security/cve/	A-SMA-ZEPH-280323/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22892		
Vendor: solidres					
Product: solidres					
Affected Version(s): * Up to (including) 0.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Mar-2023	4.8	The Solidres plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'currency_name' parameter in versions up to, and including, 0.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with administrator privileges to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-1374**	N/A	A-SOL-SOLI-280323/829
Vendor: sraoss					
Product: pg_ivm					
Affected Version(s): * Up to (excluding) 1.5.1					
Uncontrolled Search Path Element	07-Mar-2023	8.8	Uncontrolled search path element vulnerability exists in pg_ivm versions prior to 1.5.1. When refreshing an IMMV, pg_ivm executes functions without specifying schema	N/A	A-SRA-PG_I-280323/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			names. Under certain conditions, pg_ivm may be tricked to execute unexpected functions from other schemas with the IMMV owner's privilege. If this vulnerability is exploited, an unexpected function provided by an attacker may be executed with the privilege of the materialized view owner. **CVE ID : CVE-2023-23554**		
N/A	07-Mar-2023	4.3	Information disclosure vulnerability exists in pg_ivm versions prior to 1.5.1. An Incrementally Maintainable Materialized View (IMMV) created by pg_ivm may reflect rows with Row-Level Security that the owner of the IMMV should not have access to. As a result, information in tables protected by Row-Level Security may be retrieved by a user who is not authorized to access it. **CVE ID : CVE-2023-22847**	N/A	A-SRA-PG_I-280323/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: stellarium					
Product: stellarium					
Affected Version(s): * Up to (including) 1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Mar-2023	9.8	In Stellarium through 1.2, attackers can write to files that are typically unintended, such as ones with absolute pathnames or .. directory traversal. **CVE ID : CVE-2023-28371**	https://github.com/Stellarium/stellarium/commit/eba61df3b38605befcb43687a4c0a159dbc0c5cb, https://github.com/Stellarium/stellarium/commit/1261f74dc4aa6bbd01ab51434342409 7f8cf46b7	A-STE-STEL-280323/832
Vendor: stripe					
Product: stripe_payment_pro					
Affected Version(s): * Up to (excluding) 4.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Mar-2023	9.8	The PrestaShop e-commerce platform module stripejs contains a Blind SQL injection vulnerability up to version 4.5.5. The method `stripejsValidationModuleFrontController::initContent()` has sensitive SQL calls that can be executed with a trivial http call and exploited to forge a SQL injection. **CVE ID : CVE-2023-23315**	N/A	A-STR-STRI-280323/833
Vendor: struktur					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: libde265					
Affected Version(s): 1.0.10					
Out-of-bounds Write	01-Mar-2023	7.8	Libde265 v1.0.10 was discovered to contain a heap-buffer-overflow vulnerability in the derive_spatial_luma_vector_prediction function in motion.cc. **CVE ID : CVE-2023-25221**	https://github.com/strukturag/libde265/issues/388	A-STR-LIBD-280323/834
NULL Pointer Dereference	01-Mar-2023	6.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the mc_chroma function at motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24751**	https://github.com/strukturag/libde265/issues/379	A-STR-LIBD-280323/835
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_hevc_epel_pixels_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file.	https://github.com/strukturag/libde265/issues/378	A-STR-LIBD-280323/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24752		
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_weighted_pred_avg_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24754**	https://github.com/strukturag/libde265/issues/382	A-STR-LIBD-280323/837
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_weighted_pred_8_fallback function at fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24755**	https://github.com/strukturag/libde265/issues/384	A-STR-LIBD-280323/838
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_unweighted_pred_8_sse function at sse-motion.cc. This	https://github.com/strukturag/libde265/issues/380	A-STR-LIBD-280323/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24756**		
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_unweighted_pred_16_fallback function at fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24757**	https://github.com/strukturag/libde265/issues/385	A-STR-LIBD-280323/840
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_weighted_pred_avg_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24758**	https://github.com/strukturag/libde265/issues/383	A-STR-LIBD-280323/841
Affected Version(s): 1.0.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Mar-2023	8.8	Libde265 v1.0.11 was discovered to contain a heap buffer overflow via the function derive_collocated_motion_vectors at motion.cc. **CVE ID : CVE-2023-27103**	N/A	A-STR-LIBD-280323/842
NULL Pointer Dereference	15-Mar-2023	6.5	Libde265 v1.0.11 was discovered to contain a segmentation violation via the function decoder_context::process_slice_segment_header at decctx.cc. **CVE ID : CVE-2023-27102**	N/A	A-STR-LIBD-280323/843
Vendor: student_study_center_desk_management_system_project					
Product: student_study_center_desk_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-Mar-2023	7.2	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely.	N/A	A-STU-STUD-280323/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-223111. **CVE ID : CVE-2023-1407**		
Vendor: sul1ss_shop_project					
Product: sul1ss_shop					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2023	7.2	A vulnerability, which was classified as critical, has been found in SUL1SS_shop. This issue affects some unknown processing of the file application\merch\controller\Order.php. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-222599. **CVE ID : CVE-2023-1276**	N/A	A-SUL-SUL1-280323/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: swig-templates_project					
Product: swig-templates					
Affected Version(s): * Up to (including) 2.0.4					
N/A	15-Mar-2023	9.8	An issue was discovered in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to execute arbitrary code via crafted Object.prototype anonymous function. **CVE ID : CVE-2023-25344**	N/A	A-SWI-SWIG-280323/846
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-Mar-2023	7.5	Directory traversal vulnerability in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to read arbitrary files via the include or extends tags. **CVE ID : CVE-2023-25345**	N/A	A-SWI-SWIG-280323/847
Vendor: swig_project					
Product: swig					
Affected Version(s): * Up to (including) 1.4.2					
N/A	15-Mar-2023	9.8	An issue was discovered in swig-templates thru 2.0.4 and swig thru 1.4.2, allows attackers to execute arbitrary code via crafted Object.prototype anonymous function. **CVE ID : CVE-2023-25344**	N/A	A-SWI-SWIG-280323/848
Improper Limitation	15-Mar-2023	7.5	Directory traversal vulnerability in swig-	N/A	A-SWI-SWIG-280323/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			templates thru 2.0.4 and swig thru 1.4.2, allows attackers to read arbitrary files via the include or extends tags. **CVE ID : CVE-2023-25345**		
Vendor: synved					
Product: wordpress_shortcodes					
Affected Version(s): * Up to (including) 1.6.36					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The WordPress Shortcodes WordPress plugin through 1.6.36 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0063**	N/A	A-SYN-WORD-280323/850
Vendor: systemd_project					
Product: systemd					
Affected Version(s): * Up to (excluding) 247					
N/A	03-Mar-2023	7.8	systemd before 247 does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl	N/A	A-SYS-SYST-280323/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output. **CVE ID : CVE-2023-26604**		
Vendor: talentyazilim					
Product: unis					
Affected Version(s): * Up to (excluding) 28376					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	15-Mar-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Talent Software UNIS allows Reflected XSS.This issue affects UNIS: before 28376. **CVE ID : CVE-2023-0322**	N/A	A-TAL-UNIS-280323/852
Vendor: teacms_project					
Product: teacms					
Affected Version(s): 2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-Mar-2023	8.8	A vulnerability classified as critical was found in XiaoBingBy TeaCMS 2.0. Affected by this vulnerability is an unknown functionality of the file /admin/upload. The manipulation leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222985 was assigned to this vulnerability. **CVE ID : CVE-2023-1398**	N/A	A-TEA-TEAC-280323/853
Vendor: temenos					
Product: t24					
Affected Version(s): r20					
N/A	13-Mar-2023	6.5	** DISPUTED ** Incorrect access control in Temenos T24 Release 20 allows attackers to gain unauthorized access to sensitive information via a crafted POST request to HELPTEXT.MAINMENU. NOTE: the vendor's position is that "the access level granted is in line	N/A	A-TEM-T24-280323/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with business requirement." **CVE ID : CVE-2023-24368**		
Vendor: tgsoft					
Product: vir.it_explorer					
Affected Version(s): 9.4.86.0					
N/A	13-Mar-2023	5.5	A vulnerability was found in TG Soft Vir.IT eXplorer 9.4.86.0. It has been rated as problematic. This issue affects some unknown processing in the library VIRAGTLT.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 9.5 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222875. **CVE ID : CVE-2023-1369**	N/A	A-TGS-VIR.-280323/855
Product: viragtlt.sys					
Affected Version(s): 1.86.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Mar-2023	5.5	A vulnerability was found in TG Soft Vir.IT eXplorer 9.4.86.0. It has been rated as problematic. This issue affects some unknown processing in the library VIRAGTLT.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 9.5 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-222875. **CVE ID : CVE-2023-1369**	N/A	A-TGS-VIRA-280323/856
Vendor: Thekelleys					
Product: dnsmasq					
Affected Version(s): * Up to (excluding) 2.90					
N/A	15-Mar-2023	7.5	An issue was discovered in Dnsmasq before 2.90. The default maximum EDNS.0 UDP packet size was set to 4096 but should be 1232	https://thekelleys.org.uk/gitweb/?p=dnsmasq.git;a=commit;h=eb92fb32b746f2104b0f3	A-THE-DNSM-280323/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because of DNS Flag Day 2020. **CVE ID : CVE-2023-28450**	70b5b295bb8dd4bd5e5	
Vendor: thm					
Product: feedbacksystem					
Affected Version(s): * Up to (excluding) 1.5.3					
Incorrect Authorization	07-Mar-2023	4.3	thmmniii/fbs-core is an open source feedback system for students. In versions prior to 1.5.3 when querying `subresults`, it is possible to query `subresults` from other users due to insufficient authorisation. This is only possible for logged-in users and it is not possible to associate the subresults with a specific user. This bug was fixed in commit `f1ae67d8bb2`and released with version 1.5.3. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-27485**	https://github.com/thm-mni-ii/feedbacksystem/commit/f1ae67d8bb2286a8eb15949038473d41b1358493, https://github.com/thm-mni-ii/feedbacksystem/security/advisories/GHSA-fhq8-p3w6-mmgr	A-THM-FEED-280323/858
Vendor: totaljs					
Product: openplatform					
Affected Version(s): 2023-02-16					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS OpenPlatform commit b80b09d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the account name field. **CVE ID : CVE-2023-27069**	N/A	A-TOT-OPEN-280323/859
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS OpenPlatform commit b80b09d allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field. **CVE ID : CVE-2023-27070**	N/A	A-TOT-OPEN-280323/860
Vendor: trellix					
Product: intelligent_sandbox					
Affected Version(s): 5.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	6.7	A command injection vulnerability in Trellix Intelligent Sandbox CLI for version 5.2 and earlier, allows a local user to inject and execute arbitrary operating system commands using specially crafted	https://kcm.trellix.com/corporate/index?page=content&id=SB10397	A-TRE-INTE-280323/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			strings. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI command. The vulnerability allows the attack **CVE ID : CVE-2023-0978**		
Affected Version(s): 5.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	6.7	A command injection vulnerability in Trellix Intelligent Sandbox CLI for version 5.2 and earlier, allows a local user to inject and execute arbitrary operating system commands using specially crafted strings. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI command. The vulnerability allows the attack **CVE ID : CVE-2023-0978**	https://kcm.trellix.com/corporate/index?page=content&id=SB10397	A-TRE-INTE-280323/862
Vendor: Trendmicro					
Product: apex_one					
Affected Version(s): 2019					
Uncontrolled Search Path Element	10-Mar-2023	9.8	An uncontrolled search path element vulnerability in the Trend Micro Apex	https://success.trendmicro.com/solut	A-TRE-APEX-280323/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			One Server installer could allow an attacker to achieve a remote code execution state on affected products. **CVE ID : CVE-2023-25143**	ion/000292209	
N/A	10-Mar-2023	7.8	An improper access control vulnerability in the Trend Micro Apex One agent could allow a local attacker to gain elevated privileges and create arbitrary directories with arbitrary ownership. **CVE ID : CVE-2023-25144**	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/864
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A link following vulnerability in the scanning function of Trend Micro Apex One agent 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-2023-25145**	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/865
Improper Link Resolution Before File	10-Mar-2023	7.8	A security agent link following vulnerability in the Trend Micro Apex	https://success.trendmicro.com/solut	A-TRE-APEX-280323/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			One agent could allow a local attacker to quarantine a file, delete the original folder and replace with a junction to an arbitrary location, ultimately leading to an arbitrary file dropped to an arbitrary location. 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-2023-25146**	ion/000292209	
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to exploit the vulnerability by changing a specific file into a pseudo-symlink, allowing privilege escalation 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/000292209	A-TRE-APEX-280323/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25148		
Uncontrolled Search Path Element	10-Mar-2023	6.7	An issue in the Trend Micro Apex One agent could allow an attacker who has previously acquired administrative rights via other means to bypass the protection by using a specifically crafted DLL during a specific update process. Please note: an attacker must first obtain administrative access on the target system via another method in order to exploit this. **CVE ID : CVE-2023-25147**	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/868
Affected Version(s): * Up to (excluding) 14.0.11960					
Uncontrolled Search Path Element	10-Mar-2023	9.8	An uncontrolled search path element vulnerability in the Trend Micro Apex One Server installer could allow an attacker to achieve a remote code execution state on affected products. **CVE ID : CVE-2023-25143**	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/869
N/A	10-Mar-2023	7.8	An improper access control vulnerability in the Trend Micro Apex One agent could allow a local	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to gain elevated privileges and create arbitrary directories with arbitrary ownership. **CVE ID : CVE-2023-25144**		
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A link following vulnerability in the scanning function of Trend Micro Apex One agent 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-2023-25145**	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/871
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A security agent link following vulnerability in the Trend Micro Apex One agent could allow a local attacker to quarantine a file, delete the original folder and replace with a junction to an arbitrary location, ultimately leading to an arbitrary file dropped to an arbitrary location. Please note: an attacker must first obtain the ability to	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2023-25146**		
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to exploit the vulnerability by changing a specific file into a pseudo-symlink, allowing privilege escalation 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-2023-25148**	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/873
Uncontrolled Search Path Element	10-Mar-2023	6.7	An issue in the Trend Micro Apex One agent could allow an attacker who has previously acquired administrative rights via other means to bypass the protection by using a specifically crafted DLL during a specific update process. Please note: an	https://success.trendmicro.com/solution/000292209	A-TRE-APEX-280323/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker must first obtain administrative access on the target system via another method in order to exploit this. **CVE ID : CVE-2023-25147**		
Vendor: typora					
Product: typora					
Affected Version(s): * Up to (including) 1.5.5					
Improper Control of Generation of Code ('Code Injection')	07-Mar-2023	7.8	A vulnerability, which was classified as critical, was found in Typora up to 1.5.5. Affected is an unknown function of the component WSH JScript Handler. The manipulation leads to code injection. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.8 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-221736. **CVE ID : CVE-2023-1003**	N/A	A-TYP-TYPO-280323/875
Vendor: ubikasec					
Product: waap_cloud					
Affected Version(s): * Up to (excluding) 6.11.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2023	9.8	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15. **CVE ID : CVE-2023-26261**	N/A	A-UBI-WAAP-280323/876
Affected Version(s): * Up to (excluding) 6.5.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2023	9.8	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15. **CVE ID : CVE-2023-26261**	N/A	A-UBI-WAAP-280323/877
Affected Version(s): 6.5.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	08-Mar-2023	9.8	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP	N/A	A-UBI-WAAP-280323/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			Gateway & Cloud 6.11.0 and 6.5.6-patch15. **CVE ID : CVE-2023-26261**		
Product: waap_gateway					
Affected Version(s): * Up to (excluding) 6.11.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2023	9.8	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15. **CVE ID : CVE-2023-26261**	N/A	A-UBI-WAAP-280323/879
Affected Version(s): * Up to (excluding) 6.5.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2023	9.8	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15. **CVE ID : CVE-2023-26261**	N/A	A-UBI-WAAP-280323/880
Affected Version(s): 6.5.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-Mar-2023	9.8	In UBIKA WAAP Gateway/Cloud through 6.10, a blind XPath injection leads to an authentication bypass by stealing the session of another connected user. The fixed versions are WAAP Gateway & Cloud 6.11.0 and 6.5.6-patch15. **CVE ID : CVE-2023-26261**	N/A	A-UBI-WAAP-280323/881
Vendor: ubuntukylin					
Product: kylin-system-updater					
Affected Version(s): * Up to (including) 1.4.20kord					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Mar-2023	7.8	A vulnerability, which was classified as critical, was found in kylin-system-updater up to 1.4.20kord. Affected is the function InstallSnap of the component Update Handler. The manipulation leads to command injection. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222600. **CVE ID : CVE-2023-1277**	N/A	A-UBU-KYLI-280323/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ucms_project					
Product: ucms					
Affected Version(s): 1.6					
Unrestricted Upload of File with Dangerous Type	09-Mar-2023	9.8	A vulnerability was found in UCMS 1.6 and classified as critical. This issue affects some unknown processing of the file sadmin/fileedit.php of the component System File Management Module. The manipulation of the argument file leads to unrestricted upload. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-222683. **CVE ID : CVE-2023-1303**	N/A	A-UCM-UCMS-280323/883
Vendor: uvdesk					
Product: community-skeleton					
Affected Version(s): * Up to (excluding) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository uvdesk/community-skeleton prior to 1.1.0. **CVE ID : CVE-2023-1197**	https://huntr.dev/bounties/97d226ea-2cd8-4f4d-9360-aa46c37fdd26, https://github.com/uvdesk/community-skeleton/co	A-UVD-COMM-280323/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				mmit/6fae9442361c8a216611d3622bec26249a8c48a0	
Vendor: uzaybaskul					
Product: weighbridge_automation_software					
Affected Version(s): * Up to (excluding) 1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Mar-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Uzay Baskul Weighbridge Automation Software allows SQL Injection.This issue affects Weighbridge Automation Software: before 1.1. **CVE ID : CVE-2023-1064**	N/A	A-UZA-WEIG-280323/885
Vendor: vantage6					
Product: vantage6					
Affected Version(s): * Up to (excluding) 3.6.1					
Improper Preservation of Permissions	01-Mar-2023	6.5	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Assigning existing users to a different organizations is currently possible. It may lead to unintended access: if a user from organization A is	https://github.com/vantage6/vantage6/security/advisories/GHSA-vvjv-97j8-94xh, https://github.com/vantage6/vantage6/commit/798aca1de142a4eca175ef	A-VAN-VANT-280323/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accidentally assigned to organization B, they will retain their permissions and therefore might be able to access stuff they should not be allowed to access. This issue is patched in version 3.8.0. **CVE ID : CVE-2023-22738**	51112e2235642f4f24	
Affected Version(s): * Up to (excluding) 3.8.0					
Insufficient Session Expiration	04-Mar-2023	8.8	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Currently, the refresh token is valid indefinitely. The refresh token should get a validity of 24-48 hours. A fix was released in version 3.8.0. **CVE ID : CVE-2023-23929**	https://github.com/vantage6/vantage6/commit/48ebfca42359e9a6743e9598684585e2522cdce8	A-VAN-VANT-280323/887
Affected Version(s): 3.8.0					
Improper Preservation of Permissions	01-Mar-2023	6.5	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Assigning existing users to a different organizations is currently possible. It may lead to unintended access: if a user from	https://github.com/vantage6/vantage6/security/advisories/GHSA-vvjv-97j8-94xh, https://github.com/vantage6/vantage6/commit/798aca1de142a4eca175ef	A-VAN-VANT-280323/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			organization A is accidentally assigned to organization B, they will retain their permissions and therefore might be able to access stuff they should not be allowed to access. This issue is patched in version 3.8.0. **CVE ID : CVE-2023-22738**	51112e2235642f4f24	
Affected Version(s): From (including) 3.7.0 Up to (including) 3.7.3					
Improper Preservation of Permissions	01-Mar-2023	6.5	vantage6 is a privacy preserving federated learning infrastructure for secure insight exchange. Assigning existing users to a different organizations is currently possible. It may lead to unintended access: if a user from organization A is accidentally assigned to organization B, they will retain their permissions and therefore might be able to access stuff they should not be allowed to access. This issue is patched in version 3.8.0. **CVE ID : CVE-2023-22738**	https://github.com/vantage6/vantage6/security/advisories/GHSA-vvjv-97j8-94xh, https://github.com/vantage6/vantage6/commit/798aca1de142a4eca175ef51112e2235642f4f24	A-VAN-VANT-280323/889
Vendor: variscite					
Product: matrix-gui					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2023	9.8	SQL injection vulnerability found in Varisicte matrix-gui v.2 allows a remote attacker to execute arbitrary code via the shell_exect parameter to the \www\pages\matrix-gui-2.0 endpoint. **CVE ID : CVE-2023-26922**	N/A	A-VAR-MATR-280323/890
Vendor: Veeam					
Product: backup_\&_replication					
Affected Version(s): 11.0.1.1261					
Missing Authentication for Critical Function	10-Mar-2023	7.5	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts. **CVE ID : CVE-2023-27532**	https://www.veeam.com/kb4424	A-VEE-BACK-280323/891
Affected Version(s): 12.0.0.1420					
Missing Authentication for Critical Function	10-Mar-2023	7.5	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may	https://www.veeam.com/kb4424	A-VEE-BACK-280323/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to gaining access to the backup infrastructure hosts. **CVE ID : CVE-2023-27532**		
Vendor: vega-functions_project					
Product: vega-functions					
Affected Version(s): * Up to (excluding) 5.13.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2023	6.1	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. The Vega `scale` expression function has the ability to call arbitrary functions with a single controlled argument. The scale expression function passes a user supplied argument group to getScale, which is then used as if it were an internal context. The context.scales[name].value is accessed from group and called as a function back in scale. This can be exploited to escape the Vega expression sandbox in order to execute arbitrary JavaScript. This issue has been	N/A	A-VEG-VEGA-280323/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in version 5.13.1. **CVE ID : CVE-2023-26486**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2023	6.1	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs.`lassoAppend' function accepts 3 arguments and internally invokes `push` function on the 1st argument specifying array consisting of 2nd and 3rd arguments as `push` call argument. The type of the 1st argument is supposed to be an array, but it's not enforced. This makes it possible to specify any object with a `push` function as the 1st argument, `push` function can be set to any function that can be access via `event.view` (no all such functions can be exploited due to invalid context or signature, but some can, e.g. `console.log`). The issue is	https://github.com/vega/vega/commit/01adb034f24727d3bb321bbbb6696a7f4cd91689	A-VEG-VEGA-280323/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that`lassoAppend` doesn't enforce proper types of its arguments. This issue opens various XSS vectors, but exact impact and severity depends on the environment (e.g. Core JS `setImmediate` polyfill basically allows `eval`-like functionality). This issue was patched in 5.23.0. **CVE ID : CVE-2023-26487**		
Vendor: vega_project					
Product: vega					
Affected Version(s): * Up to (excluding) 5.23.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2023	6.1	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. The Vega `scale` expression function has the ability to call arbitrary functions with a single controlled argument. The scale expression function passes a user supplied argument group to getScale, which is then used as if it were an internal	N/A	A-VEG-VEGA-280323/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context. The context.scales[name] .value is accessed from group and called as a function back in scale. This can be exploited to escape the Vega expression sandbox in order to execute arbitrary JavaScript. This issue has been fixed in version 5.13.1. **CVE ID : CVE-2023-26486**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2023	6.1	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs.`lassoAppend' function accepts 3 arguments and internally invokes `push` function on the 1st argument specifying array consisting of 2nd and 3rd arguments as `push` call argument. The type of the 1st argument is supposed to be an array, but it's not enforced. This makes it possible to specify any object with a `push` function as the 1st argument,	https://github.com/vega/vega/commit/01adb034f24727d3bb321bbbb6696a7f4cd91689	A-VEG-VEGA-280323/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`push` function can be set to any function that can be access via `event.view` (no all such functions can be exploited due to invalid context or signature, but some can, e.g. `console.log`). The issue is that`lassoAppend` doesn't enforce proper types of its arguments. This issue opens various XSS vectors, but exact impact and severity depends on the environment (e.g. Core JS `setImmediate` polyfill basically allows `eval`-like functionality). This issue was patched in 5.23.0. **CVE ID : CVE-2023-26487**		
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.1367					
Divide By Zero	01-Mar-2023	7.8	Divide By Zero in GitHub repository vim/vim prior to 9.0.1367. **CVE ID : CVE-2023-1127**	https://github.com/vim/vim/commit/e0f869196930ef5f25a0ac41c9215b09c9ce2d3c, https://hunt r.dev/bounti	A-VIM-VIM-280323/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				es/2d4d309e-4c96-415f-9070-36d0815f1beb	
Affected Version(s): * Up to (excluding) 9.0.1376					
Heap-based Buffer Overflow	03-Mar-2023	6.6	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1376. **CVE ID : CVE-2023-1170**	https://github.com/vim/vim/commit/1c73b65229c25e3c1fd8824ba958f7cc4d604f9c, https://hunt r.dev/bounties/286e0090-e654-46d2-ac60-29f81799d0a4	A-VIM-VIM-280323/898
Affected Version(s): * Up to (excluding) 9.0.1378					
Incorrect Calculation of Buffer Size	04-Mar-2023	6.6	Incorrect Calculation of Buffer Size in GitHub repository vim/vim prior to 9.0.1378. **CVE ID : CVE-2023-1175**	https://github.com/vim/vim/commit/c99cbf8f289bdda5d4a77d7ec415850a520330ba, https://hunt r.dev/bounties/7e93fc17-92eb-4ae7-b01a-93bb460b643e	A-VIM-VIM-280323/899
Affected Version(s): * Up to (excluding) 9.0.1392					
NULL Pointer Dereference	07-Mar-2023	5.5	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.1392.	https://hunt r.dev/bounties/b2989095-88f3-413a-9a39-c1c58a6e68	A-VIM-VIM-280323/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1264	15, https://github.com/vim/vim/commit/7ac5023a5f1a37baafbe1043645f97ba3443d9f6	
Affected Version(s): * Up to (excluding) 9.0.1402					
NULL Pointer Dereference	11-Mar-2023	5.5	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.1402. **CVE ID : CVE-2023-1355**	https://github.com/vim/vim/commit/d13dd30240e32071210f55b587182ff48757ea46, https://huntr.dev/bounties/4d0a9615-d438-4f5c-8dd6-aa22f4b716d9	A-VIM-VIM-280323/901
Vendor: vxcontrol					
Product: soldr					
Affected Version(s): 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	5.4	SOLDR (System of Orchestration, Lifecycle control, Detection and Response) 1.1.0 allows stored XSS via the module editor. **CVE ID : CVE-2023-26608**	N/A	A-VXC-SOLD-280323/902
Vendor: wallabag					
Product: wallabag					
Affected Version(s): * Up to (excluding) 2.5.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	05-Mar-2023	5.3	Improper Authorization in GitHub repository wallabag/wallabag prior to 2.5.4. **CVE ID : CVE-2023-0734**	https://hunter.dev/bounties/a296324c-6925-4f5f-a729-39b0d73d5b8b, https://github.com/wallabag/wallabag/commit/acd285dcbb71b595e6320bb1d0d3a44cdf646ac0	A-WAL-WALL-280323/903
Vendor: Web2py					
Product: web2py					
Affected Version(s): * Up to (excluding) 2.23.1					
URL Redirection to Untrusted Site ('Open Redirect')	06-Mar-2023	6.1	Open redirect vulnerability exists in web2py versions prior to 2.23.1. When using the tool, a web2py user may be redirected to an arbitrary website by accessing a specially crafted URL. As a result, the user may become a victim of a phishing attack. **CVE ID : CVE-2023-22432**	N/A	A-WEB-WEB2-280323/904
Vendor: webassembly					
Product: webassembly					
Affected Version(s): 1.0.29					
Out-of-bounds Write	10-Mar-2023	7.8	WebAssembly v1.0.29 was discovered to contain a heap overflow via the	N/A	A-WEB-WEBA-280323/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component component wabt::Node::operator. **CVE ID : CVE-2023-27117**		
N/A	10-Mar-2023	5.5	WebAssembly v1.0.29 was discovered to contain a segmentation fault via the component wabt::cat_compute_size. **CVE ID : CVE-2023-27115**	N/A	A-WEB-WEBA-280323/906
N/A	10-Mar-2023	5.5	WebAssembly v1.0.29 discovered to contain an abort in CWriter::MangleType. **CVE ID : CVE-2023-27116**	N/A	A-WEB-WEBA-280323/907
N/A	10-Mar-2023	5.5	WebAssembly v1.0.29 was discovered to contain a segmentation fault via the component wabt::Decompiler::WrapChild. **CVE ID : CVE-2023-27119**	N/A	A-WEB-WEBA-280323/908
Vendor: webhostings					
Product: wh_testimonials					
Affected Version(s): * Up to (including) 3.0.0					
Improper Neutralization of Input	13-Mar-2023	6.1	The WH Testimonials plugin for WordPress is vulnerable to Stored	N/A	A-WEB-WH_T-280323/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting via several parameters such as wh_homepage, wh_text_short, wh_text_full and in versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-1372**		
Vendor: Webkitgtk					
Product: webkitgtk					
Affected Version(s): * Up to (excluding) 2.36.8					
Use After Free	02-Mar-2023	9.8	A use-after-free vulnerability in WebCore::RenderLayer::addChild in WebKitGTK before 2.36.8 allows attackers to execute code remotely. **CVE ID : CVE-2023-25358**	https://bugs.webkit.org/show_bug.cgi?id=242683	A-WEB-WEBK-280323/910
Use After Free	02-Mar-2023	9.8	A use-after-free vulnerability in WebCore::RenderLayer::renderer in WebKitGTK before 2.36.8 allows	https://bugs.webkit.org/show_bug.cgi?id=242686	A-WEB-WEBK-280323/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute code remotely. **CVE ID : CVE-2023-25360**		
Use After Free	02-Mar-2023	9.8	A use-after-free vulnerability in WebCore::RenderLayer::setNextSibling in WebKitGTK before 2.36.8 allows attackers to execute code remotely. **CVE ID : CVE-2023-25361**	https://bugs.webkit.org/show_bug.cgi?id=244249	A-WEB-WEBK-280323/912
Use After Free	02-Mar-2023	9.8	A use-after-free vulnerability in WebCore::RenderLayer::repaintBlockSelectionGaps in WebKitGTK before 2.36.8 allows attackers to execute code remotely. **CVE ID : CVE-2023-25362**	https://bugs.webkit.org/show_bug.cgi?id=244802	A-WEB-WEBK-280323/913
Use After Free	02-Mar-2023	9.8	A use-after-free vulnerability in WebCore::RenderLayer::updateDescendantDependentFlags in WebKitGTK before 2.36.8 allows attackers to execute code remotely. **CVE ID : CVE-2023-25363**	https://bugs.webkit.org/show_bug.cgi?id=242684	A-WEB-WEBK-280323/914
Vendor: webpack.js					
Product: webpack					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.76.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	13-Mar-2023	9.8	Webpack 5 before 5.76.0 does not avoid cross-realm object access. ImportParserPlugin.js mishandles the magic comment feature. An attacker who controls a property of an untrusted object can obtain access to the real global object. **CVE ID : CVE-2023-28154**	https://github.com/webpack/webpack/compare/v5.75.0...v5.76.0, https://github.com/webpack/webpack/pull/16500	A-WEB-WEBP-280323/915
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.12					
N/A	06-Mar-2023	7.1	ISO 15765 and ISO 10681 dissector crash in Wireshark 4.0.0 to 4.0.3 and 3.6.0 to 3.6.11 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-1161**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1161.json, https://gitlab.com/wireshark/wireshark/-/issues/18839, https://www.wireshark.org/security/wnpa-sec-2023-08.html	A-WIR-WIRE-280323/916
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.4					
N/A	06-Mar-2023	7.1	ISO 15765 and ISO 10681 dissector crash in Wireshark 4.0.0 to 4.0.3 and	https://gitlab.com/gitlab-org/cves/-/blob/maste	A-WIR-WIRE-280323/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.6.0 to 3.6.11 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-1161**	r/2023/CVE-2023-1161.json, https://gitlab.com/wireshark/wireshark/-/issues/18839, https://www.wireshark.org/security/wnpa-sec-2023-08.html	
Vendor: wisecleaner					
Product: wise_folder_hider					
Affected Version(s): 4.4.3.202					
Improper Resource Shutdown or Release	06-Mar-2023	5.5	A vulnerability was found in WiseCleaner Wise Folder Hider 4.4.3.202. It has been declared as problematic. Affected by this vulnerability is an unknown functionality in the library WiseFs64.sys of the component IoControlCode Handler. The manipulation leads to denial of service. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-222361 was	N/A	A-WIS-WISE-280323/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-1189**		
Vendor: wondershare					
Product: dr.phone					
Affected Version(s): 12.9.6					
N/A	13-Mar-2023	7.8	Wondershare Dr.Fone v12.9.6 was discovered to contain weak permissions for the service WsDrvInst. This vulnerability allows attackers to escalate privileges via modifying or overwriting the executable. **CVE ID : CVE-2023-27010**	N/A	A-WON-DR.P-280323/919
Vendor: wow-company					
Product: bubble_menu					
Affected Version(s): * Up to (excluding) 3.0.2					
Cross-Site Request Forgery (CSRF)	01-Mar-2023	5.4	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Bubble Menu – circle floating menu plugin <= 3.0.1 leading to form deletion. **CVE ID : CVE-2023-23984**	N/A	A-WOW-BUBB-280323/920
Vendor: wpaudio_mp3_player_project					
Product: wpaudio_mp3_player					
Affected Version(s): * Up to (including) 4.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Mar-2023	5.4	The WPaudio MP3 Player WordPress plugin through 4.0.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0069**	N/A	A-WPA-WPAU-280323/921
Vendor: wpcode					
Product: wpcode					
Affected Version(s): * Up to (excluding) 2.0.7					
Incorrect Authorization	06-Mar-2023	4.3	The WPCode WordPress plugin before 2.0.7 does not have adequate privilege checks in place for several AJAX actions, only checking the nonce. This may lead to allowing any authenticated user who can edit posts to call the endpoints related to WPCode Library authentication (such as update and delete the auth key). **CVE ID : CVE-2023-0328**	N/A	A-WPC-WPCO-280323/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpmanageninja					
Product: fluentsmtp					
Affected Version(s): * Up to (excluding) 2.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Mar-2023	5.4	The FluentSMTP WordPress plugin before 2.2.3 does not sanitize or escape email content, making it vulnerable to stored cross-site scripting attacks (XSS) when an administrator views the email logs. This exploit requires other plugins to enable users to send emails with unfiltered HTML. **CVE ID : CVE-2023-0219**	N/A	A-WPM-FLUE-280323/923
Vendor: wpmet					
Product: metform_elementor_contact_form_builder					
Affected Version(s): * Up to (including) 3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	6.1	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via text areas on forms in versions up to, and including, 3.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2845078%40metform&new=2845078%40metform&sfp_email=&sfph_mail=	A-WPM-METF-280323/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in pages that will execute whenever a user accesses an injected page, which is the submissions page. **CVE ID : CVE-2023-0084**		
Affected Version(s): * Up to (including) 3.2.1					
Protection Mechanism Failure	02-Mar-2023	5.3	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to reCaptcha Bypass in versions up to, and including, 3.2.1. This is due to insufficient server side checking on the captcha value submitted during a form submission. This makes it possible for unauthenticated attackers to bypass Captcha restrictions and for attackers to utilize bots to submit forms. **CVE ID : CVE-2023-0085**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2868889%40metform&new=2868889%40metform&sfp_email=&sfph_mail=	A-WPM-METF-280323/925
Vendor: xcat_project					
Product: xcat					
Affected Version(s): * Up to (excluding) 2.16.5					
Incorrect Authorization	08-Mar-2023	8.8	xCAT is a toolkit for deployment and administration of computer clusters. In versions prior to 2.16.5 if zones are	https://github.com/xcat2/xcat-core/security/advisories/GHSA-hpxg-	A-XCA-XCAT-280323/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured as a mechanism to secure clusters in XCAT, it is possible for a local root user from one node to obtain credentials to SSH to any node in any zone, except the management node of the default zone. XCAT zones are not enabled by default. Only users that use the optional zone feature are impacted. All versions of xCAT prior to xCAT 2.16.5 are vulnerable. This problem has been fixed in xCAT 2.16.5. Users making use of zones should upgrade to 2.16.5. Users unable to upgrade may mitigate the issue by disabling zones or patching the management node with the fix contained in commit `85149c37f49`. **CVE ID : CVE-2023-27486**	7428-6jvv, https://github.com/xcat2/xcat-core/pull/7247/commits/85149c37f49dbca7bd85f1f586960315604fc024, https://github.com/xcat2/xcat-core/pull/7247	
Vendor: xhcms_project					
Product: xhcms					
Affected Version(s): 1.0					
Improper Neutralization of Special	13-Mar-2023	9.8	A vulnerability was found in XHCMS 1.0. It has been declared as critical. This	N/A	A-XHC-XHCM-280323/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			vulnerability affects unknown code of the file login.php of the component POST Parameter Handler. The manipulation of the argument user leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222874 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1368**		
Vendor: xjd2020					
Product: fastcms					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Mar-2023	7.2	A vulnerability classified as problematic has been found in fastcms. This affects an unknown part of the file admin/TemplateController.java of the component ZIP File Handler. The manipulation leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use	https://github.com/my-fastcms/fastcms/issues/1	A-XJD-FAST-280323/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-222363. **CVE ID : CVE-2023-1191**		
Vendor: Xwiki					
Product: commons					
Affected Version(s): 3.1					
N/A	02-Mar-2023	9.9	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1. **CVE ID : CVE-2023-26055**	https://jira.xwiki.org/browse/XWIKI-19793, https://jira.xwiki.org/browse/XWIKI-19794, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-8cw6-4r32-6r3h, https://jira.xwiki.org/browse/XCOMMONS-2498	A-XWI-COMM-280323/929
Affected Version(s): 3.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Mar-2023	9.9	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1. **CVE ID : CVE-2023-26055**	https://jira.xwiki.org/browse/XWIKI-19793, https://jira.xwiki.org/browse/XWIKI-19794, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-8cw6-4r32-6r3h, https://jira.xwiki.org/browse/XCOMMONS-2498	A-XWI-COMM-280323/930
Affected Version(s): 14.4					
N/A	02-Mar-2023	9.9	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all	https://jira.xwiki.org/browse/XWIKI-19793, https://jira.xwiki.org/browse/XWIKI-19794, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-8cw6-4r32-	A-XWI-COMM-280323/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1. **CVE ID : CVE-2023-26055**	6r3h, https://jira.xwiki.org/browse/XCOMMONS-2498	
Affected Version(s): From (including) 14.4 Up to (excluding) 14.4.4					
N/A	02-Mar-2023	9.9	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1. **CVE ID : CVE-2023-26055**	https://jira.xwiki.org/browse/XWIKI-19793, https://jira.xwiki.org/browse/XWIKI-19794, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-8cw6-4r32-6r3h, https://jira.xwiki.org/browse/XCOMMONS-2498	A-XWI-COMM-280323/932
Affected Version(s): From (including) 14.5 Up to (excluding) 14.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Mar-2023	9.9	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1. **CVE ID : CVE-2023-26055**	https://jira.xwiki.org/browse/XWIKI-19793, https://jira.xwiki.org/browse/XWIKI-19794, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-8cw6-4r32-6r3h, https://jira.xwiki.org/browse/XCOMMONS-2498	A-XWI-COMM-280323/933
Affected Version(s): From (including) 3.2 Up to (excluding) 13.10.9					
N/A	02-Mar-2023	9.9	XWiki Commons are technical libraries common to several other top level XWiki projects. Starting in version 3.1-milestone-1, any user can edit their own profile and inject code, which is going to be executed with programming right. The same vulnerability can also be exploited in all	https://jira.xwiki.org/browse/XWIKI-19793, https://jira.xwiki.org/browse/XWIKI-19794, https://github.com/xwiki/xwiki-commons/security/advisories/GHSA-8cw6-4r32-	A-XWI-COMM-280323/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other places where short text properties are displayed, e.g., in apps created using Apps Within Minutes that use a short text field. The problem has been patched on versions 13.10.9, 14.4.4, 14.7RC1. **CVE ID : CVE-2023-26055**	6r3h, https://jira.xwiki.org/browse/XCOMMONS-2498	
Product: Xwiki					
Affected Version(s): 3.2					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch manually on `LiveTableResults` and `WikisLiveTableResultsMacros`. **CVE ID : CVE-2023-26476**	https://jira.xwiki.org/browse/XWIKI-19949, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5cf8-vrr8-8hjm, https://github.com/xwiki/xwiki-platform/commit/7f8825537c9523ccb5051abd78014d156f9791c8	A-XWI-XWIK-280323/935
Affected Version(s): * Up to (excluding) 14.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to make the farm unusable by adding an object to a page with a huge number (e.g. 67108863). Most of the time this will fill the memory allocated to XWiki and make it unusable every time this document is manipulated. This issue has been patched in XWiki 14.0-rc-1. **CVE ID : CVE-2023-26470**	https://github.com/xwiki/xwiki-platform/commit/fdfce062642b0ac062da5cda033d25482f4600fa, https://github.com/xwiki/xwiki-platform/commit/db3d1c62fc5fb59fefcda3b86065d2d362f55164, https://jira.xwiki.org/browse/XWIKI-19223	A-XWI-XWIK-280323/936
Affected Version(s): 1.1					
Improper Restriction of XML External Entity Reference	07-Mar-2023	7.7	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit rights on a document can trigger an XAR import on a forged XAR file, leading to the ability to display the content of any file on the XWiki server host. This vulnerability has been patched in XWiki 13.10.11,	https://github.com/xwiki/xwiki-platform/commit/e3527b98fdd8dc8179c24dc55e662b2c55199434, https://jira.xwiki.org/browse/XWIKI-20320, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-	A-XWI-XWIK-280323/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.4.7 and 14.10-rc-1. Users are advised to upgrade. Users unable to upgrade may apply the patch `e3527b98fd` manually. **CVE ID : CVE-2023-27480**	gx4f-976g-7g6v	
Affected Version(s): 1.3					
N/A	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 1.3-rc-1, any user with edit right can execute arbitrary database select and access data stored in the database. The problem has been patched in XWiki 13.10.11, 14.4.7, and 14.10. There is no workaround for this vulnerability other than upgrading. **CVE ID : CVE-2023-26473**	https://jira.xwiki.org/browse/XWIKI-19523, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vpx4-7rfp-h545	A-XWI-XWIK-280323/938
Affected Version(s): 11.6					
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 11.6-rc-1, comments are supposed to be executed with the right of superadmin but in restricted mode (anything dangerous is disabled), but the async macro does	https://github.com/xwiki/xwiki-platform/commit/00532d9f1404287cf3ec3a05056640d809516006, https://github.com/xwiki/xwiki-platform/sec	A-XWI-XWIK-280323/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not take into account the restricted mode. This means that any user with comment right can use the async macro to make it execute any wiki content with the right of superadmin. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10. The only known workaround consists of applying a patch and rebuilding and redeploying `org.xwiki.platform:xwiki-platform-rendering-async-macro`. **CVE ID : CVE-2023-26471**	urity/advisories/GHSA-9cqm-5wf7-wcj7, https://jira.xwiki.org/browse/XWIKI-20234	
Affected Version(s): 14.7					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch	https://jira.xwiki.org/browse/XWIKI-19949, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5cf8-vrr8-8hjm, https://github.com/xwiki/xwiki-platform/commit/7f8825537c9523ccb5051abd7	A-XWI-XWIK-280323/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manually on `LiveTableResults` and `WikisLiveTableResultsMacros`. **CVE ID : CVE-2023-26476**	8014d156f9791c8	
Affected Version(s): 14.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 12.10, a user without script rights can introduce a stored cross-site scripting by using the Live Data macro. This has been patched in XWiki 14.9, 14.4.7, and 13.10.10. There are no known workarounds. **CVE ID : CVE-2023-26480**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-32fq-m2q5-h83g, https://github.com/xwiki/xwiki-platform/commit/556e7823260b826f344c1a6e95d935774587e028, https://jira.xwiki.org/browse/XWIKI-20143	A-XWI-XWIK-280323/941
Affected Version(s): 2.3					
Improper Privilege Management	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 2.3-milestone-1, the annotation displayer does not execute the content in a restricted context. This allows executing anything with the right of the	https://github.com/xwiki/xwiki-platform/commit/d87d7bfd8db18c20d3264f98c6deefeae93b99f7, https://jira.xwiki.org/browse/XWIKI-	A-XWI-XWIK-280323/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			author of any document by annotating the document. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. There is no easy workaround except to upgrade. **CVE ID : CVE-2023-26475**	20360, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-h6f5-8jj5-cxhr, https://jira.xwiki.org/browse/XWIKI-20384	
Affected Version(s): 3.0					
Incorrect Authorization	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 3.0-milestone-1, it's possible to execute a script with the right of another user, provided the target user does not have programming right. The problem has been patched in XWiki 14.8-rc-1, 14.4.5, and 13.10.10. There are no known workarounds for this issue. **CVE ID : CVE-2023-26056**	https://github.com/xwiki/xwiki-platform/commit/4b75f212c2dd2dfc5fb5726c7830c6dbc9a425c6, https://github.com/xwiki/xwiki-platform/commit/bd34ad6710ed72304304a3d5fec38b7cc050ef3b, https://jira.xwiki.org/browse/XWIKI-19856	A-XWI-XWIK-280323/943
Affected Version(s): 6.2					
Improper Encoding or Escaping of Output	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute any wiki	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-	A-XWI-XWIK-280323/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af2b531026a614221d5d61f38. **CVE ID : CVE-2023-26472**	vwr6-qp4q-2wj7, https://github.com/xwiki/xwiki-platform/commit/48caf7491595238af2b531026a614221d5d61f38#diff-2ec9d716673ee049937219cdb0a92e520f81da14ea84d144504b97ab2bdae243R45	
Affected Version(s): 6.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Mar-2023	9.9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qxjg-jhgw-qhrv, https://jira.xwiki.org/browse/XWIKI-20294, https://github.com/xwiki	A-XWI-XWIK-280323/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause is improper escaping of UIX parameters. A proof of concept exploit is to log in, add an `XWiki.UIExtensionClass` xobject to the user profile page, with an Extension Parameters content containing `label={{/html}}{{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("Hello " + "from groovy!"){{/groovy}}{{/async}}`. Then, navigating to `PanelsCode.ApplicationsPanelConfigurationSheet` (i.e., `<xwiki-host>/xwiki/bin/view/PanelsCode/ApplicationsPanelConfigurationSheet` where `<xwiki-host>` is the URL of your XWiki installation) should not execute the Groovy script. If it does, you will see `Hello from groovy!` displayed on the screen. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. For users unable to upgrade	/xwiki-platform/commit/6de5442f3c91c3634a66c7b458d5b142e1c2a2dc	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the issue can be fixed by editing the `PanelsCode.ApplicationsPanelConfigurationSheet` wiki page and making the same modifications as shown in commit `6de5442f3c`. **CVE ID : CVE-2023-27479**		
Affected Version(s): From (excluding) 1.1 Up to (excluding) 13.10.11					
Improper Restriction of XML External Entity Reference	07-Mar-2023	7.7	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit rights on a document can trigger an XAR import on a forged XAR file, leading to the ability to display the content of any file on the XWiki server host. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. Users unable to upgrade may apply the patch `e3527b98fd` manually. **CVE ID : CVE-2023-27480**	https://github.com/xwiki/xwiki-platform/commit/e3527b98fdd8dc8179c24dc55e662b2c55199434, https://jira.xwiki.org/browse/XWIKI-20320, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gx4f-976g-7g6v	A-XWI-XWIK-280323/946
Affected Version(s): From (excluding) 2.3 Up to (excluding) 13.10.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 2.3-milestone-1, the annotation displayer does not execute the content in a restricted context. This allows executing anything with the right of the author of any document by annotating the document. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. There is no easy workaround except to upgrade. **CVE ID : CVE-2023-26475**	https://github.com/xwiki/xwiki-platform/commit/d87d7bfd8db18c20d3264f98c6deefeae93b99f7, https://jira.xwiki.org/browse/XWIKI-20360, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-h6f5-8jj5-cxhr, https://jira.xwiki.org/browse/XWIKI-20384	A-XWI-XWIK-280323/947
Affected Version(s): From (excluding) 6.3 Up to (excluding) 13.10.11					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Mar-2023	9.9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of UIX parameters. A proof	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qxjg-jhgw-qhrv, https://jira.xwiki.org/browse/XWIKI-20294, https://github.com/xwiki/xwiki-platform/commit/6de54	A-XWI-XWIK-280323/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of concept exploit is to log in, add an `XWiki.UIExtensionClass` xobject to the user profile page, with an Extension Parameters content containing `label={{/html}}{{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("Hello " + "from groovy!"){{/groovy}}{{/async}}`. Then, navigating to `PanelsCode.ApplicationsPanelConfigurationSheet` (i.e., `<xwiki-host>/xwiki/bin/view/PanelsCode/ApplicationsPanelConfigurationSheet` where `<xwiki-host>` is the URL of your XWiki installation) should not execute the Groovy script. If it does, you will see `Hello from groovy!` displayed on the screen. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. For users unable to upgrade the issue can be fixed by editing the `PanelsCode.Applicat	42f3c91c3634a66c7b458d5b142e1c2a2dc	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ionsPanelConfigurationSheet` wiki page and making the same modifications as shown in commit `6de5442f3c`. **CVE ID : CVE-2023-27479**		
Affected Version(s): From (including) 1.3 Up to (excluding) 13.10.11					
N/A	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 1.3-rc-1, any user with edit right can execute arbitrary database select and access data stored in the database. The problem has been patched in XWiki 13.10.11, 14.4.7, and 14.10. There is no workaround for this vulnerability other than upgrading. **CVE ID : CVE-2023-26473**	https://jira.xwiki.org/browse/XWIKI-19523, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vpx4-7rfp-h545	A-XWI-XWIK-280323/949
Affected Version(s): From (including) 11.6 Up to (excluding) 13.10.10					
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 11.6-rc-1, comments are supposed to be executed with the right of superadmin but in restricted mode (anything dangerous is disabled), but the async macro does not take into account	https://github.com/xwiki/xwiki-platform/commit/00532d9f1404287cf3ec3a05056640d809516006, https://github.com/xwiki/xwiki-platform/security/adviso	A-XWI-XWIK-280323/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the restricted mode. This means that any user with comment right can use the async macro to make it execute any wiki content with the right of superadmin. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10. The only known workaround consists of applying a patch and rebuilding and redeploying `org.xwiki.platform:xwiki-platform-rendering-async-macro`. **CVE ID : CVE-2023-26471**	ries/GHSA-9cqm-5wf7-wcj7, https://jira.xwiki.org/browse/XWIKI-20234	
Affected Version(s): From (including) 12.10 Up to (excluding) 13.10.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 12.10, a user without script rights can introduce a stored cross-site scripting by using the Live Data macro. This has been patched in XWiki 14.9, 14.4.7, and 13.10.10. There are no known workarounds. **CVE ID : CVE-2023-26480**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-32fq-m2q5-h83g, https://github.com/xwiki/xwiki-platform/commit/556e7823260b826f344c1a6e95d935774587e028, https://jira.xwiki.org/bro	A-XWI-XWIK-280323/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				wse/XWIKI-20143	
Affected Version(s): From (including) 13.10 Up to (excluding) 13.10.11					
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 13.10, it's possible to use the right of an existing document content author to execute a text area property. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11. There are no known workarounds. **CVE ID : CVE-2023-26474**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3738-p9x3-mv9r, https://jira.xwiki.org/browse/XWIKI-20373	A-XWI-XWIK-280323/952
Affected Version(s): From (including) 13.5.0 Up to (excluding) 13.10.9					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch manually on `LiveTableResults`	https://jira.xwiki.org/browse/XWIKI-19949, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5cf8-vrr8-8hjm, https://github.com/xwiki/xwiki-platform/commit/7f8825537c9523ccb5051abd78014d156f9791c8	A-XWI-XWIK-280323/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and `WikisLiveTableResultsMacros`. **CVE ID : CVE-2023-26476**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.5					
Incorrect Authorization	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 3.0-milestone-1, it's possible to execute a script with the right of another user, provided the target user does not have programming right. The problem has been patched in XWiki 14.8-rc-1, 14.4.5, and 13.10.10. There are no known workarounds for this issue. **CVE ID : CVE-2023-26056**	https://github.com/xwiki/xwiki-platform/commit/4b75f212c2dd2dfc5fb5726c7830c6dbc9a425c6, https://github.com/xwiki/xwiki-platform/commit/bd34ad6710ed72304304a3d5fec38b7cc050ef3b, https://jira.xwiki.org/browse/XWIKI-19856	A-XWI-XWIK-280323/954
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.6					
Improper Control of Generation of Code ('Code Injection')	02-Mar-2023	9.8	XWiki Platform is a generic wiki platform. Starting in versions 6.3-rc-1 and 6.2.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the `newThemeName` request parameter (URL parameter), in	https://github.com/xwiki/xwiki-platform/commit/ea2e615f50a918802fd60b09ec87aa04bc6ea8e2#diff-e2153fa59f9d92ef67b0afbf27984bd17170921a3b	A-XWI-XWIK-280323/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			combination with additional parameters. This has been patched in the supported versions 13.10.10, 14.9-rc-1, and 14.4.6. As a workaround, it is possible to edit `FlamingoThemesCode.WebHomeSheet` and manually perform the changes from the patch fixing the issue. **CVE ID : CVE-2023-26477**	558fac227160003d0dfd2aR283-R284, https://jira.xwiki.org/browse/XWIKI-19757	
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 11.6-rc-1, comments are supposed to be executed with the right of superadmin but in restricted mode (anything dangerous is disabled), but the async macro does not take into account the restricted mode. This means that any user with comment right can use the async macro to make it execute any wiki content with the right of superadmin. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10. The only	https://github.com/xwiki/xwiki-platform/commit/00532d9f1404287cf3ec3a05056640d809516006, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9cqm-5wf7-wcj7, https://jira.xwiki.org/browse/XWIKI-20234	A-XWI-XWIK-280323/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workaround consists of applying a patch and rebuilding and redeploying `org.xwiki.platform:xwiki-platform-rendering-async-macro`. **CVE ID : CVE-2023-26471**		
Improper Encoding or Escaping of Output	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute any wiki content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af2b531026a614221d5d61f38.	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vwr6-qp4q-2wj7, https://github.com/xwiki/xwiki-platform/commit/48caf7491595238af2b531026a614221d5d61f38#diff-2ec9d716673ee049937219cdb0a92e520f81da14ea84d144504b97ab2bdae243R45	A-XWI-XWIK-280323/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26472		
Improper Handling of Exceptional Conditions	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 6.0, users with write rights can insert well-formed content that is not handled well by the parser. As a consequence, some pages becomes unusable, including the user index (if the page containing the faulty content is a user page) and the page index. Note that on the page, the normal UI is completely missing and it is not possible to open the editor directly to revert the change as the stack overflow is already triggered while getting the title of the document. This means that it is quite difficult to remove this content once inserted. This has been patched in XWiki 13.10.10, 14.4.6, and 14.9-rc-1. A temporary workaround to avoid Stack Overflow errors is to increase the memory allocated to the stack by using the `-Xss`	https://jira.xwiki.org/browse/XWIKI-19838, https://github.com/xwiki/xwiki-platform/commit/e5b82cd98072464196a468b8f7fe6396dce142a7, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-52vf-hvv3-98h7	A-XWI-XWIK-280323/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JVM parameter (e.g., `-Xss32m`). This should allow the parser to pass and to fix the faulty content. The consequences for other aspects of the system (e.g., performance) are unknown, and this workaround should be only be used as a temporary solution. The workaround does not prevent the issue occurring again with other content. Consequently, it is strongly advised to upgrade to a version where the issue has been patched. **CVE ID : CVE-2023-26479**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.7					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Mar-2023	9.9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of UIX parameters. A proof of concept exploit is	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qxjg-jhgw-qhrv, https://jira.xwiki.org/browse/XWIKI-20294, https://github.com/xwiki/xwiki-platform/commit/6de5442f3c91c363	A-XWI-XWIK-280323/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to log in, add an `XWiki.UIExtensionClass` xobject to the user profile page, with an Extension Parameters content containing `label={{/html}}{{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("Hello " + "from groovy!"){{/groovy}}{{/async}}`. Then, navigating to `PanelsCode.ApplicationsPanelConfigurationSheet` (i.e., `<xwiki-host>/xwiki/bin/view/PanelsCode/ApplicationsPanelConfigurationSheet` where `<xwiki-host>` is the URL of your XWiki installation) should not execute the Groovy script. If it does, you will see `Hello from groovy!` displayed on the screen. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. For users unable to upgrade the issue can be fixed by editing the `PanelsCode.ApplicationsPanelConfigurati	4a66c7b458d5b142e1c2a2dc	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			onSheet` wiki page and making the same modifications as shown in commit `6de5442f3c`. **CVE ID : CVE-2023-27479**		
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 13.10, it's possible to use the right of an existing document content author to execute a text area property. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11. There are no known workarounds. **CVE ID : CVE-2023-26474**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3738-p9x3-mv9r, https://jira.xwiki.org/browse/XWIKI-20373	A-XWI-XWIK-280323/960
Improper Privilege Management	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 2.3-milestone-1, the annotation displayer does not execute the content in a restricted context. This allows executing anything with the right of the author of any document by annotating the document. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10.	https://github.com/xwiki/xwiki-platform/commit/d87d7bfd8db18c20d3264f98c6deefeae93b99f7, https://jira.xwiki.org/browse/XWIKI-20360, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-	A-XWI-XWIK-280323/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There is no easy workaround except to upgrade. **CVE ID : CVE-2023-26475**	h6f5-8jj5-cxhr, https://jira.xwiki.org/browse/XWIKI-20384	
Improper Restriction of XML External Entity Reference	07-Mar-2023	7.7	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit rights on a document can trigger an XAR import on a forged XAR file, leading to the ability to display the content of any file on the XWiki server host. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. Users unable to upgrade may apply the patch `e3527b98fd` manually. **CVE ID : CVE-2023-27480**	https://github.com/xwiki/xwiki-platform/commit/e3527b98fdd8dc8179c24dc55e662b2c55199434, https://jira.xwiki.org/browse/XWIKI-20320, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gx4f-976g-7g6v	A-XWI-XWIK-280323/962
N/A	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 1.3-rc-1, any user with edit right can execute arbitrary database select and access data stored in the database. The	https://jira.xwiki.org/browse/XWIKI-19523, https://github.com/xwiki/xwiki-platform/security/adviso	A-XWI-XWIK-280323/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problem has been patched in XWiki 13.10.11, 14.4.7, and 14.10. There is no workaround for this vulnerability other than upgrading. **CVE ID : CVE-2023-26473**	ries/GHSA-vpx4-7rfp-h545	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 12.10, a user without script rights can introduce a stored cross-site scripting by using the Live Data macro. This has been patched in XWiki 14.9, 14.4.7, and 13.10.10. There are no known workarounds. **CVE ID : CVE-2023-26480**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-32fq-m2q5-h83g, https://github.com/xwiki/xwiki-platform/commit/556e7823260b826f344c1a6e95d935774587e028, https://jira.xwiki.org/browse/XWIKI-20143	A-XWI-XWIK-280323/964
Affected Version(s): From (including) 14.0 Up to (excluding) 14.7					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue	https://jira.xwiki.org/browse/XWIKI-19949, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5cf8-vrr8-8hjm,	A-XWI-XWIK-280323/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch manually on `LiveTableResults` and `WikisLiveTableResultsMacros`. **CVE ID : CVE-2023-26476**	https://github.com/xwiki/xwiki-platform/commit/7f8825537c9523ccb5051abd78014d156f9791c8	
Affected Version(s): From (including) 14.3 Up to (excluding) 14.4.6					
N/A	02-Mar-2023	8.1	XWiki Platform is a generic wiki platform. Starting in version 14.3-rc-1, `org.xwiki.store.script.TemporaryAttachmentsScriptService#uploadTemporaryAttachment` returns an instance of `com.xpn.xwiki.doc.XWikiAttachment`. This class is not supported to be exposed to users without the `programing` right. `com.xpn.xwiki.api.Attachment` should be used instead and takes case of checking the user's rights before performing dangerous operations. This has been patched in versions 14.9-rc-1	https://jira.xwiki.org/browse/XWIKI-20180, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-8692-g6g9-gm5p, https://github.com/xwiki/xwiki-platform/commit/3c73c59e39b6436b1074d8834cf276916010014d	A-XWI-XWIK-280323/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 14.4.6. There are no known workarounds for this issue. **CVE ID : CVE-2023-26478**		
Affected Version(s): From (including) 14.5 Up to (excluding) 14.10					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Mar-2023	9.9	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of UIX parameters. A proof of concept exploit is to log in, add an `XWiki.UIExtensionClass` xobject to the user profile page, with an Extension Parameters content containing `label={{/html}}{{async async="true" cached="false" context="doc.reference"}}{{groovy}}println("Hello " + "from groovy!"){{/groovy}}{{/async}}`. Then, navigating to `PanelsCode.ApplicationsPanelConfigurati	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qxjg-jhgw-qhrv, https://jira.xwiki.org/browse/XWIKI-20294, https://github.com/xwiki/xwiki-platform/commit/6de5442f3c91c3634a66c7b458d5b142e1c2a2dc	A-XWI-XWIK-280323/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			onSheet` (i.e., `<xwiki-host>/xwiki/bin/view/PanelsCode/ApplicationsPanelConfigurationSheet` where `<xwiki-host>` is the URL of your XWiki installation) should not execute the Groovy script. If it does, you will see `Hello from groovy!` displayed on the screen. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. For users unable to upgrade the issue can be fixed by editing the `PanelsCode.ApplicationsPanelConfigurationSheet` wiki page and making the same modifications as shown in commit `6de5442f3c`. **CVE ID : CVE-2023-27479**		
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 13.10, it's possible to use the right of an existing document content author to execute a text area property. This has been	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3738-p9x3-mv9r, https://jira.xwiki.org/bro	A-XWI-XWIK-280323/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in XWiki 14.10, 14.4.7, and 13.10.11. There are no known workarounds. **CVE ID : CVE-2023-26474**	wse/XWIKI-20373	
Improper Privilege Management	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 2.3-milestone-1, the annotation displayer does not execute the content in a restricted context. This allows executing anything with the right of the author of any document by annotating the document. This has been patched in XWiki 13.10.11, 14.4.7 and 14.10. There is no easy workaround except to upgrade. **CVE ID : CVE-2023-26475**	https://github.com/xwiki/xwiki-platform/commit/d87d7bfd8db18c20d3264f98c6deefeae93b99f7, https://jira.xwiki.org/browse/XWIKI-20360, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-h6f5-8jj5-cxhr, https://jira.xwiki.org/browse/XWIKI-20384	A-XWI-XWIK-280323/969
Improper Restriction of XML External Entity Reference	07-Mar-2023	7.7	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit rights on a document can trigger an XAR import on a forged	https://github.com/xwiki/xwiki-platform/commit/e3527b98fdd8dc8179c24dc55e662b2c55199434, https://jira.xwiki.org/bro	A-XWI-XWIK-280323/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XAR file, leading to the ability to display the content of any file on the XWiki server host. This vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10-rc-1. Users are advised to upgrade. Users unable to upgrade may apply the patch `e3527b98fd` manually. **CVE ID : CVE-2023-27480**	wse/XWIKI-20320, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gx4f-976g-7g6v	
N/A	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 1.3-rc-1, any user with edit right can execute arbitrary database select and access data stored in the database. The problem has been patched in XWiki 13.10.11, 14.4.7, and 14.10. There is no workaround for this vulnerability other than upgrading. **CVE ID : CVE-2023-26473**	https://jira.xwiki.org/browse/XWIKI-19523, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vpx4-7rfp-h545	A-XWI-XWIK-280323/971
Affected Version(s): From (including) 14.5 Up to (excluding) 14.8					
Incorrect Authorization	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 3.0-milestone-1, it's possible to execute a	https://github.com/xwiki/xwiki-platform/commit/4b75f212c2dd2dfc	A-XWI-XWIK-280323/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			script with the right of another user, provided the target user does not have programming right. The problem has been patched in XWiki 14.8-rc-1, 14.4.5, and 13.10.10. There are no known workarounds for this issue. **CVE ID : CVE-2023-26056**	5fb5726c7830c6dbc9a425c6, https://github.com/xwiki/xwiki-platform/commit/bd34ad6710ed72304304a3d5fec38b7cc050ef3b, https://jira.xwiki.org/browse/XWIKI-19856	
Affected Version(s): From (including) 14.5 Up to (excluding) 14.9					
Improper Control of Generation of Code ('Code Injection')	02-Mar-2023	9.8	XWiki Platform is a generic wiki platform. Starting in versions 6.3-rc-1 and 6.2.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the `newThemeName` request parameter (URL parameter), in combination with additional parameters. This has been patched in the supported versions 13.10.10, 14.9-rc-1, and 14.4.6. As a workaround, it is possible to edit `FlamingoThemesCode.WebHomeSheet` and manually perform the changes	https://github.com/xwiki/xwiki-platform/commit/ea2e615f50a918802fd60b09ec87aa04bc6ea8e2#diff-e2153fa59f9d92ef67b0afbf27984bd17170921a3b558fac227160003d0dfd2aR283-R284, https://jira.xwiki.org/browse/XWIKI-19757	A-XWI-XWIK-280323/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the patch fixing the issue. **CVE ID : CVE-2023-26477**		
N/A	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 11.6-rc-1, comments are supposed to be executed with the right of superadmin but in restricted mode (anything dangerous is disabled), but the async macro does not take into account the restricted mode. This means that any user with comment right can use the async macro to make it execute any wiki content with the right of superadmin. This has been patched in XWiki 14.9, 14.4.6, and 13.10.10. The only known workaround consists of applying a patch and rebuilding and redeploying `org.xwiki.platform:xwiki-platform-rendering-async-macro`. **CVE ID : CVE-2023-26471**	https://github.com/xwiki/xwiki-platform/commit/00532d9f1404287cf3ec3a05056640d809516006, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9cqm-5wf7-wcj7, https://jira.xwiki.org/browse/XWIKI-20234	A-XWI-XWIK-280323/974
Improper Encoding or	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in	https://github.com/xwiki/xwiki-	A-XWI-XWIK-280323/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			version 6.2-milestone-1, one can execute any wiki content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af2b531026a614221d5d61f38. **CVE ID : CVE-2023-26472**	platform/security/advisories/GHSA-vwr6-qp4q-2wj7, https://github.com/xwiki/xwiki-platform/commit/48caf7491595238af2b531026a614221d5d61f38#diff-2ec9d716673ee049937219cdb0a92e520f81da14ea84d144504b97ab2bdae243R45	
N/A	02-Mar-2023	8.1	XWiki Platform is a generic wiki platform. Starting in version 14.3-rc-1, `org.xwiki.store.script.TemporaryAttachmentsScriptService#uploadTemporaryAttachment` returns an instance of `com.xpn.xwiki.doc.XWikiAttachment`.	https://jira.xwiki.org/browse/XWIKI-20180, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-8692-g6g9-gm5p,	A-XWI-XWIK-280323/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This class is not supported to be exposed to users without the `programing` right. `com.xpn.xwiki.api.Attachment` should be used instead and takes case of checking the user's rights before performing dangerous operations. This has been patched in versions 14.9-rc-1 and 14.4.6. There are no known workarounds for this issue. **CVE ID : CVE-2023-26478**	https://github.com/xwiki/xwiki-platform/commit/3c73c59e39b6436b1074d8834cf276916010014d	
Improper Handling of Exceptional Conditions	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 6.0, users with write rights can insert well-formed content that is not handled well by the parser. As a consequence, some pages becomes unusable, including the user index (if the page containing the faulty content is a user page) and the page index. Note that on the page, the normal UI is completely missing and it is not possible	https://jira.xwiki.org/browse/XWIKI-19838, https://github.com/xwiki/xwiki-platform/commit/e5b82cd98072464196a468b8f7fe6396dce142a7, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-52vf-hvv3-98h7	A-XWI-XWIK-280323/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to open the editor directly to revert the change as the stack overflow is already triggered while getting the title of the document. This means that it is quite difficult to remove this content once inserted. This has been patched in XWiki 13.10.10, 14.4.6, and 14.9-rc-1. A temporary workaround to avoid Stack Overflow errors is to increase the memory allocated to the stack by using the `-Xss` JVM parameter (e.g., `-Xss32m`). This should allow the parser to pass and to fix the faulty content. The consequences for other aspects of the system (e.g., performance) are unknown, and this workaround should be only be used as a temporary solution. The workaround does not prevent the issue occurring again with other content. Consequently, it is strongly advised to upgrade to a version where the issue has been patched.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26479		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 12.10, a user without script rights can introduce a stored cross-site scripting by using the Live Data macro. This has been patched in XWiki 14.9, 14.4.7, and 13.10.10. There are no known workarounds. **CVE ID : CVE-2023-26480**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-32fq-m2q5-h83g, https://github.com/xwiki/xwiki-platform/commit/556e7823260b826f344c1a6e95d935774587e028, https://jira.xwiki.org/browse/XWIKI-20143	A-XWI-XWIK-280323/978
Affected Version(s): From (including) 3.1 Up to (excluding) 13.10.10					
Incorrect Authorization	02-Mar-2023	5.4	XWiki Platform is a generic wiki platform. Starting in version 3.0-milestone-1, it's possible to execute a script with the right of another user, provided the target user does not have programming right. The problem has been patched in XWiki 14.8-rc-1, 14.4.5, and 13.10.10. There are no known workarounds for this issue.	https://github.com/xwiki/xwiki-platform/commit/4b75f212c2dd2dfc5fb5726c7830c6dbc9a425c6, https://github.com/xwiki/xwiki-platform/commit/bd34ad6710ed72304304a3d5fec38b7cc050ef3b, https://jira.x	A-XWI-XWIK-280323/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26056	wiki.org/browse/XWIKI-19856	
Affected Version(s): From (including) 3.3 Up to (excluding) 13.4.4					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	7.5	XWiki Platform is a generic wiki platform. Starting in version 3.2-m3, users can deduce the content of the password fields by repeated call to `LiveTableResults` and `WikisLiveTableResultsMacros`. The issue can be fixed by upgrading to versions 14.7-rc-1, 13.4.4, or 13.10.9 and higher, or in version >= 3.2M3 by applying the patch manually on `LiveTableResults` and `WikisLiveTableResultsMacros`. **CVE ID : CVE-2023-26476**	https://jira.xwiki.org/browse/XWIKI-19949, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5cf8-vrr8-8hjm, https://github.com/xwiki/xwiki-platform/commit/7f8825537c9523ccb5051abd78014d156f9791c8	A-XWI-XWIK-280323/980
Affected Version(s): From (including) 6.0 Up to (excluding) 13.10.10					
Improper Handling of Exceptional Conditions	02-Mar-2023	6.5	XWiki Platform is a generic wiki platform. Starting in version 6.0, users with write rights can insert well-formed content that is not handled well by the parser. As a consequence, some pages becomes	https://jira.xwiki.org/browse/XWIKI-19838, https://github.com/xwiki/xwiki-platform/commit/e5b82cd98072464196a468b8f	A-XWI-XWIK-280323/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unusable, including the user index (if the page containing the faulty content is a user page) and the page index. Note that on the page, the normal UI is completely missing and it is not possible to open the editor directly to revert the change as the stack overflow is already triggered while getting the title of the document. This means that it is quite difficult to remove this content once inserted. This has been patched in XWiki 13.10.10, 14.4.6, and 14.9-rc-1. A temporary workaround to avoid Stack Overflow errors is to increase the memory allocated to the stack by using the `-Xss` JVM parameter (e.g., `-Xss32m`). This should allow the parser to pass and to fix the faulty content. The consequences for other aspects of the system (e.g., performance) are unknown, and this workaround should be only be used as a temporary solution.	7fe6396dce142a7, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-52vf-hvv3-98h7	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The workaround does not prevent the issue occurring again with other content. Consequently, it is strongly advised to upgrade to a version where the issue has been patched. **CVE ID : CVE-2023-26479**		
Affected Version(s): From (including) 6.2.1 Up to (excluding) 13.10.10					
Improper Encoding or Escaping of Output	02-Mar-2023	8.8	XWiki Platform is a generic wiki platform. Starting in version 6.2-milestone-1, one can execute any wiki content with the right of IconThemeSheet author by creating an icon theme with certain content. This can be done by creating a new page or even through the user profile for users not having edit right. The issue has been patched in XWiki 14.9, 14.4.6, and 13.10.10. An available workaround is to fix the bug in the page `IconThemesCode.IconThemeSheet` by applying a modification from commit 48caf7491595238af	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vwr6-qp4q-2wj7, https://github.com/xwiki/xwiki-platform/commit/48caf7491595238af2b531026a614221d5d61f38#diff-2ec9d716673ee049937219cdb0a92e520f81da14ea84d144504b97ab2bdae243R45	A-XWI-XWIK-280323/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2b531026a614221d5d61f38. **CVE ID : CVE-2023-26472**		
Affected Version(s): From (including) 6.2.4 Up to (excluding) 13.10.10					
Improper Control of Generation of Code ('Code Injection')	02-Mar-2023	9.8	XWiki Platform is a generic wiki platform. Starting in versions 6.3-rc-1 and 6.2.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the `newThemeName` request parameter (URL parameter), in combination with additional parameters. This has been patched in the supported versions 13.10.10, 14.9-rc-1, and 14.4.6. As a workaround, it is possible to edit `FlamingoThemesCode.WebHomeSheet` and manually perform the changes from the patch fixing the issue. **CVE ID : CVE-2023-26477**	https://github.com/xwiki/xwiki-platform/commit/ea2e615f50a918802fd60b09ec87aa04bc6ea8e2#diff-e2153fa59f9d92ef67b0afbf27984bd17170921a3b558fac227160003d0dfd2aR283-R284, https://jira.xwiki.org/browse/XWIKI-19757	A-XWI-XWIK-280323/983
Vendor: yf-exam_project					
Product: yf-exam					
Affected Version(s): 1.8.0					
Deserialization of	03-Mar-2023	9.8	CleverStupidDog yf-exam v 1.8.0 is vulnerable to	N/A	A-YF--YF-E-280323/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			Deserialization which can lead to remote code execution (RCE). **CVE ID : CVE-2023-26779**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Mar-2023	9.8	CleverStupidDog yf-exam v 1.8.0 is vulnerable to SQL Injection. **CVE ID : CVE-2023-26780**	N/A	A-YF--YF-E-280323/985
Unrestricted Upload of File with Dangerous Type	03-Mar-2023	7.5	CleverStupidDog yf-exam 1.8.0 is vulnerable to File Upload. There is no restriction on the suffix of the uploaded file, resulting in any file upload. **CVE ID : CVE-2023-25402**	N/A	A-YF--YF-E-280323/986
Authorization Bypass Through User-Controlled Key	03-Mar-2023	7.5	CleverStupidDog yf-exam v 1.8.0 is vulnerable to Authentication Bypass. The program uses a fixed JWT key, and the stored key uses username format characters. Any user who logged in within 24 hours. A token can be forged with his username to bypass authentication.	N/A	A-YF--YF-E-280323/987

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25403		
Vendor: yoga_class_registration_system_project					
Product: yoga_class_registration_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Mar-2023	7.2	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been classified as critical. This affects the function query of the file admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-222873 was assigned to this vulnerability. **CVE ID : CVE-2023-1366**	N/A	A-YOG-YOGA-280323/988
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Mar-2023	6.1	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been declared as problematic. This vulnerability affects the function query of the file admin/user/list.php.	N/A	A-YOG-YOGA-280323/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-222982 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1395**		
Vendor: Zohocorp					
Product: manageengine_assetexplorer					
Affected Version(s): * Up to (excluding) 6.9					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/990
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports.	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26600		
Affected Version(s): 6.9					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/992
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports. **CVE ID : CVE-2023-26600**	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/993
Product: manageengine_servicedesk_plus					
Affected Version(s): * Up to (excluding) 14.1					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**		
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports. **CVE ID : CVE-2023-26600**	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/995
Affected Version(s): 14.1					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/996
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege escalation via query reports. **CVE ID : CVE-2023-26600**		
Product: manageengine_servicedesk_plus_msp					
Affected Version(s): * Up to (excluding) 14.0					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/998
Affected Version(s): * Up to (excluding) 13.0					
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports. **CVE ID : CVE-2023-26600**	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/999
Affected Version(s): 13.0					
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and	https://www.manageengine.com/products/service-desk/CVE-	A-ZOH-MANA-280323/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Asset Explorer through 6987 allow privilege escalation via query reports. **CVE ID : CVE-2023-26600**	2023-26600.html	
Affected Version(s): 14.0					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/1001
Product: manageengine_supportcenter_plus					
Affected Version(s): * Up to (excluding) 14.0					
Uncontrolled Resource Consumption	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987, ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	https://www.manageengine.com/products/service-desk/CVE-2023-26601.html	A-ZOH-MANA-280323/1002
Affected Version(s): 14.0					
Uncontrolled Resource	06-Mar-2023	7.5	Zoho ManageEngine ServiceDesk Plus through 14104, Asset Explorer through 6987,	https://www.manageengine.com/products/service-	A-ZOH-MANA-280323/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			ServiceDesk Plus MSP before 14000, and Support Center Plus before 14000 allow Denial-of-Service (DoS). **CVE ID : CVE-2023-26601**	desk/CVE-2023-26601.html	
Affected Version(s): * Up to (excluding) 11.0					
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports. **CVE ID : CVE-2023-26600**	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/1004
Affected Version(s): 11.0					
N/A	06-Mar-2023	6.5	ManageEngine ServiceDesk Plus through 14104, ServiceDesk Plus MSP through 14000, Support Center Plus through 14000, and Asset Explorer through 6987 allow privilege escalation via query reports. **CVE ID : CVE-2023-26600**	https://www.manageengine.com/products/service-desk/CVE-2023-26600.html	A-ZOH-MANA-280323/1005
Vendor: \@nubosoftware\/node-static_project					
Product: \@nubosoftware\/node-static					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Mar-2023	7.5	All versions of the package @nubosoftware/node-static; all versions of the package node-static are vulnerable to Directory Traversal due to improper file path sanitization in the startsWith() method in the servePath function. **CVE ID : CVE-2023-26111**	N/A	A-\@N-\@NU-280323/1006
Hardware					
Vendor: akuvox					
Product: e11					
Affected Version(s): -					
Use of Hard-coded Credentials	13-Mar-2023	9.8	The Akuvox E11 secure shell (SSH) server is enabled by default and can be accessed by the root user. This password cannot be changed by the user. **CVE ID : CVE-2023-0345**	N/A	H-AKU-E11-290323/1007
Storing Passwords in a Recoverable Format	13-Mar-2023	9.8	Akuvox E11 uses a weak encryption algorithm for stored passwords and uses a hard-coded password for decryption which could allow the encrypted passwords to be decrypted from the configuration file.	N/A	H-AKU-E11-290323/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0353		
Missing Authorization	13-Mar-2023	9.1	The Akuvox E11 libvoice library provides unauthenticated access to the camera capture for image and video. This could allow an attacker to view and record image and video from the camera. **CVE ID : CVE-2023-0349**	N/A	H-AKU-E11-290323/1009
Weak Password Recovery Mechanism for Forgotten Password	13-Mar-2023	9.1	The Akuvox E11 password recovery webpage can be accessed without authentication, and an attacker could download the device key file. An attacker could then use this page to reset the password back to the default. **CVE ID : CVE-2023-0352**	N/A	H-AKU-E11-290323/1010
Missing Authentication for Critical Function	13-Mar-2023	9.1	The Akuvox E11 web server can be accessed without any user authentication, and this could allow an attacker to access sensitive information, as well as create and download packet captures with known default URLs.	N/A	H-AKU-E11-290323/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0354		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	8.8	The Akuvox E11 web server backend library allows command injection in the device phone-book contacts functionality. This could allow an attacker to upload files with executable command instructions. **CVE ID : CVE-2023-0351**	N/A	H-AKU-E11-290323/1012
Improper Authentication	13-Mar-2023	7.5	Akuvox E11 cloud login is performed through an unencrypted HTTP connection. An attacker could gain access to the Akuvox cloud and device if the MAC address of a device if known. **CVE ID : CVE-2023-0346**	N/A	H-AKU-E11-290323/1013
N/A	13-Mar-2023	7.5	Akuvox E11 allows direct SIP calls. No access control is enforced by the SIP servers, which could allow an attacker to contact any device within Akuvox to call any other device. **CVE ID : CVE-2023-0348**	N/A	H-AKU-E11-290323/1014
Use of Hard-coded	13-Mar-2023	7.5	Akuvox E11 uses a hard-coded cryptographic key,	N/A	H-AKU-E11-290323/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Key			which could allow an attacker to decrypt sensitive information. **CVE ID : CVE-2023-0355**		
Insufficient Verification of Data Authenticity	13-Mar-2023	6.5	Akuvox E11 does not ensure that a file extension is associated with the file provided. This could allow an attacker to upload a file to the device by changing the extension of a malicious file to an accepted file type. **CVE ID : CVE-2023-0350**	N/A	H-AKU-E11-290323/1016
N/A	13-Mar-2023	5.3	The Akuvox E11 Media Access Control (MAC) address, a primary identifier, combined with the Akuvox E11 IP address, could allow an attacker to identify the device on the Akuvox cloud. **CVE ID : CVE-2023-0347**	N/A	H-AKU-E11-290323/1017
Vendor: apsystems					
Product: energy_communication_unit					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an	14-Mar-2023	9.8	OS command injection affects Altenergy Power Control Software C1.2.5 via shell metacharacters in	N/A	H-APS-ENER-290323/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			the index.php/management/set_timezone timezone parameter, because of set_timezone in models/management_model.php. **CVE ID : CVE-2023-28343**		
Vendor: Arubanetworks					
Product: 7010					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1019
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22763**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1021
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1022
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1024
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1026
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1027
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the underlying operating system. **CVE ID : CVE-2023-22773**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1029
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1030
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7010-290323/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**		
Product: 7030					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1032
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22763		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1034
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1035
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1037
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1038
Improper Neutralizat	01-Mar-2023	7.2	Authenticated command injection	https://www.arubanetw	H-ARU-7030-290323/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	orks.com/assets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1040
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22773		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1042
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1043
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7030-290323/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**		
Product: 7205					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1045
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1047
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1048
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1050
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1051
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-7205-290323/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1053
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1055
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1056
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7205-290323/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the impacted account **CVE ID : CVE-2023-22771**		
Product: 7210					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1058
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1059
Improper Neutralization of	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist	https://www.arubanetworks.com/as	H-ARU-7210-290323/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1061
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1063
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1064
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1066
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1067
Improper Limitation	01-Mar-2023	6.5	Authenticated path traversal	https://www.arubanetw	H-ARU-7210-290323/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	orks.com/assets/alert/ARUBA-PSA-2023-002.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1069
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7210-290323/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22771		
Product: 7220					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1071
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1072
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/A	H-ARU-7220-290323/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1074
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1076
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1077
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1079
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1080
Improper Limitation of a Pathname to a Restricted Directory	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1082
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7220-290323/1083
Product: 7240xm					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1084
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1085
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1087
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1088
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-7240-290323/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1090
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22769		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1092
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1093
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the underlying operating system. **CVE ID : CVE-2023-22774**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1095
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7240-290323/1096
Product: 7280					
Affected Version(s): -					
Improper Neutralization of	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist	https://www.arubanetworks.com/as	H-ARU-7280-290323/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1098
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22764**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1100
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1101
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1103
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1105
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1106
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22774		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1108
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-7280-290323/1109
Product: 9004					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/A	H-ARU-9004-290323/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1111
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1113
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1114
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1116
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1117
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-9004-290323/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	RUBA-PSA-2023-002.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1119
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1120
Improper Limitation of a	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists	https://www.arubanetworks.com/as	H-ARU-9004-290323/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	sets/alert/ARUBA-PSA-2023-002.txt	
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1122
Product: 9004-lte					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1124
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1125
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-9004-290323/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1127
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22767		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1129
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1130
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1132
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1133
Improper Limitation of a Pathname to a Restricted	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9004-290323/1135
Product: 9012					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22762		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1137
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1138
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1140
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1141
Improper Neutralizat	01-Mar-2023	7.2	Authenticated command injection	https://www.arubanetw	H-ARU-9012-290323/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	orks.com/assets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1143
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22770**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1145
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1146
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-9012-290323/1148
Product: mc-va-10					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1150
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1151
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1153
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1154
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MC-V-290323/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1156
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22770		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1158
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1159
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system files. **CVE ID : CVE-2023-22776**		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1161
Product: mc-va-1k					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1162
Improper Neutralization of	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist	https://www.arubanetworks.com/as	H-ARU-MC-V-290323/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1164
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22765**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1166
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1167
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1169
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1171
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1172
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22776		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1174
Product: mc-va-250					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1175
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/A	H-ARU-MC-V-290323/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1177
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1179
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1180
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1182
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1183
Improper Limitation of a Pathname to a	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MC-V-290323/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	RUBA-PSA-2023-002.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1185
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1186
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists	https://www.arubanetworks.com/as	H-ARU-MC-V-290323/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	sets/alert/ARUBA-PSA-2023-002.txt	
Product: mc-va-50					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1188
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1190
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1191
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MC-V-290323/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1193
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22768		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1195
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1196
Improper Limitation of a Pathname to a Restricted Directory	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1198
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1199
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MC-V-290323/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**		
Product: mcr-hw-10k					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1201
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22763		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1203
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1204
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1206
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1207
Improper Neutralizat	01-Mar-2023	7.2	Authenticated command injection	https://www.arubanetw	H-ARU-MCR--290323/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	orks.com/assets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1209
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22773		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1211
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1212
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**		
Product: mcr-hw-1k					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1214
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1216
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1217
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1219
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1220
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--290323/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1222
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1224
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1225
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the impacted account **CVE ID : CVE-2023-22771**		
Product: mcr-hw-5k					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1227
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1228
Improper Neutralization of	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist	https://www.arubanetworks.com/as	H-ARU-MCR--290323/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1230
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22766**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1232
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1233
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1235
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1236
Improper Limitation	01-Mar-2023	6.5	Authenticated path traversal	https://www.arubanetw	H-ARU-MCR--290323/1237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	orks.com/assets/alert/ARUBA-PSA-2023-002.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1238
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22771		
Product: mcr-va-10k					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1240
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1241
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--290323/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1243
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1245
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1246
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1248
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1249
Improper Limitation of a Pathname to a Restricted Directory	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1251
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1252
Product: mcr-va-1k					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1253
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1254
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1256
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1257
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--290323/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1259
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22769		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1261
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1262
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the underlying operating system. **CVE ID : CVE-2023-22774**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1264
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1265
Product: mcr-va-50					
Affected Version(s): -					
Improper Neutralization of	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist	https://www.arubanetworks.com/as	H-ARU-MCR--290323/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1267
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22764**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1269
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1270
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1272
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1274
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1275
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22774		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1277
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1278
Product: mcr-va-500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--290323/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1280
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1282
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1283
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1285
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1286
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--290323/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	RUBA-PSA-2023-002.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1288
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1289
Improper Limitation of a	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists	https://www.arubanetworks.com/as	H-ARU-MCR--290323/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	sets/alert/ARUBA-PSA-2023-002.txt	
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1291
Product: mcr-va-5k					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1293
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1294
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line	https://www.arubanetworks.com/assets/alert/A	H-ARU-MCR--290323/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1296
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22767		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1298
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1299
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1301
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1302
Improper Limitation of a Pathname to a Restricted	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	H-ARU-MCR--290323/1304
Vendor: baicells					
Product: eg7035-m11					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	Baicells EG7035-M11 devices with firmware through BCE-ODU-1.0.8 are vulnerable to improper code exploitation via HTTP GET command injections. Commands are executed using pre-login execution and executed with root	N/A	H-BAI-EG70-290323/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions. The following methods have been tested and validated by a 3rd party analyst and have been confirmed exploitable special thanks to Lionel Musonza for the discovery. **CVE ID : CVE-2023-1097**		
Vendor: Barracuda					
Product: t100b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	H-BAR-T100-290323/1306
Product: t193a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	H-BAR-T193-290323/1307
Product: t200c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	H-BAR-T200-290323/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**		
Product: t400c					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	H-BAR-T400-290323/1309
Product: t600d					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/rele	H-BAR-T600-290323/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	ase-notes-8-3-1/	
Product: t900b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters.	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	H-BAR-T900-290323/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26213		
Product: t93a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	H-BAR-T93A-290323/1312
Vendor: bbraun					
Product: battery-pack_sp_with_wifi					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	13-Mar-2023	7.2	An improper neutralization of directives in dynamically evaluated code vulnerability in the WiFi Battery embedded web server in versions L90/U70 and	N/A	H-BBR-BATT-290323/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			L92/U92 can be used to gain administrative access to the WiFi communication module. An authenticated user, having access to both the medical device WiFi network (such as a biomedical engineering staff member) and the specific B.Braun Battery Pack SP with WiFi web server credentials, could get administrative (root) access on the infusion pump communication module. This could be used as a vector to start further attacks **CVE ID : CVE-2023-0888**		
Vendor: Cisco					
Product: asr_9000v-v2					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-	H-CIS-ASR_-290323/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	load-infodisc-9rdOr5Fq	
Product: asr_9001					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-ASR_-290323/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	visory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	
Product: asr_9006					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-ASR_-290323/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**	sa-bfd-XmRescbT	
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR	https://sec.cloudapps.cisco.com/security/center/	H-CIS-ASR_-290323/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	
Product: asr_9010					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	H-CIS-ASR_-290323/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**	visory/cisco-sa-bfd-XmRescbT	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1321
Product: asr_9901					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: asr_9902					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20064		
Product: asr_9903					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: asr_9904					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: asr_9906					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: asr_9910					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: asr_9912					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: asr_9922					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	H-CIS-ASR_-290323/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-ASR_-290323/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ios_xrv_9000					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-IOS_-290323/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ip_phone_6825					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1339
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_6841					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1341
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_6851					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1343
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_6861					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1345
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_6871					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1347
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_7811					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1349
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_7821					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1351
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_7832					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1353
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_7841					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1355
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_7861					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1357
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_8811					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1359
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-	H-CIS-IP_P-290323/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	cmd-inj-KMFynVcP	
Product: ip_phone_8831					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1361
Product: ip_phone_8832					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-IP_P-290323/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	oSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1363
Product: ip_phone_8841					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-IP_P-290323/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	oSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1365
Product: ip_phone_8845					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-IP_P-290323/1366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	oSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1367
Product: ip_phone_8851					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-IP_P-290323/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	oSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1369
Product: ip_phone_8861					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-IP_P-290323/1370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	oSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1371
Product: ip_phone_8865					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-IP_P-290323/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	oSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-IP_P-290323/1373
Product: nc57-18dd-se					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow	https://sec.cloudapps.cisco.com/security/center/content/Cisc	H-CIS-NC57-290323/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	oSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	
Product: nc57-24dd					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-NC57-290323/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	sa-iosxr-load-infodisc-9rdOr5Fq	
Product: nc57-36h-se					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-	H-CIS-NC57-290323/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	infodisc-9rdOr5Fq	
Product: nc57-36h6d-s					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-	H-CIS-NC57-290323/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	infodisc-9rdOr5Fq	
Product: ncs_1001					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_1002					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_1004					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5001					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5002					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5011					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_540					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_540_fronthaul					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5501					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5501-se					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5502					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5502-se					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5508					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_5516					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_560-4					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_560-7					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_57b1-5dse-sys					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_57b1-6d24-sys					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_57c1-48q6-sys					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_57c3-mod-sys					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_57c3-mods-sys					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: ncs_6000					
Affected Version(s): -					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	H-CIS-NCS_-290323/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks against the device. **CVE ID : CVE-2023-20064**		
Product: unified_ip_phone_7945g					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-UNIF-290323/1400
Product: unified_ip_phone_7965g					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-UNIF-290323/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**		
Product: unified_ip_phone_7975g					
Affected Version(s): -					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	H-CIS-UNIF-290323/1402
Vendor: Dlink					
Product: dir-820l					
Affected Version(s): a1					
Improper Neutralization of Special Elements used in an OS Command ('OS	13-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload.	https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20In%20tools_	H-DLI-DIR--290323/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			**CVE ID : CVE-2023-25279**	AccountName	
Out-of-bounds Write	13-Mar-2023	7.5	A stack overflow vulnerability in D-Link DIR820LA1_FW106B02 allows attackers to cause a denial of service via the reserveDHCP_HostName_1.1.1.0 parameter to lan.asp. **CVE ID : CVE-2023-25283**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--290323/1404
Out-of-bounds Write	15-Mar-2023	6.5	A heap overflow vulnerability in D-Link DIR820LA1_FW106B02 allows attackers to cause a denial of service via the config.log_to_syslog and log_opt_dropPackets parameters to mydlink_api.ccp. **CVE ID : CVE-2023-25282**	https://www.dlink.com/en/security-bulletin/, https://github.com/migraine-sudo/D_Link_Vuln/tree/main/Permanent%20DDOS%20vulnerability%20in%20emailInfo	H-DLI-DIR--290323/1405
Product: dir-867					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR-867 DIR_867_FW1.30B07 allows attackers to execute arbitrary commands via a crafted LocalIPAddress parameter for the	N/A	H-DLI-DIR--290323/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SetVirtualServerSettings to HNAP1. **CVE ID : CVE-2023-24762**		
Vendor: Draytek					
Product: vigor130					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1407
Product: vigor165					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1408
Product: vigor166					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	H-DRA-VIGO-290323/1409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2133					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2133ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2133fvac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2133n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1413
Product: vigor2133vac					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1414
Product: vigor2135					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	H-DRA-VIGO-290323/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: vigor2135ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2135ax					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2135fvac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: vigor2135vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1419
Product: vigor2762					
Affected Version(s): -					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	H-DRA-VIGO-290323/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2762ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2762n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2762vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2763					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1424
Product: vigor2763ac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1425
Product: vigor2765					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	H-DRA-VIGO-290323/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2765ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2765ax					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2765va					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2766					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1430
Product: vigor2766ac					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1431
Product: vigor2766ax					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	H-DRA-VIGO-290323/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: vigor2766vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2832					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2832n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: vigor2860					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1436
Product: vigor2860ac					
Affected Version(s): -					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	H-DRA-VIGO-290323/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2860l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860ln					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860n-plus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1441
Product: vigor2860vac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1442
Product: vigor2860vn-plus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	H-DRA-VIGO-290323/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability -(cve-2023-23313)/	
Product: vigor2960					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Mar-2023	7.8	DrayTek Vigor2960 v1.5.1.4 was discovered to contain a command injection vulnerability via the mainfunction.cgi component. **CVE ID : CVE-2023-24229**	N/A	H-DRA-VIGO-290323/1444
Product: vigornic_132					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIGO-290323/1445
Product: vigor_2960					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	03-Mar-2023	8.8	A vulnerability, which was classified as critical, was found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1225C of the file	N/A	H-DRA-VIGO-290323/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			mainfunction.cgi. The manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222258 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1162**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Mar-2023	6.5	A vulnerability has been found in DrayTek Vigor 2960 1.5.1.4 and classified as problematic. Affected by this vulnerability is the function sub_1DA58 of the file mainfunction.cgi. The manipulation leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222259. **CVE ID : CVE-2023-1163**	N/A	H-DRA-VIGO-290323/1447
Product: virgor1000b					
Affected Version(s): -					
Improper Neutralizat	03-Mar-2023	6.1	Certain Draytek products are	https://www.draytek.co	H-DRA-VIRG-290323/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	m/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2862					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	H-DRA-VIRG-290323/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2862ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862b					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862bn					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: virgor2862l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1453
Product: virgor2862lac					
Affected Version(s): -					
Improper Neutralization of Input During	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi	https://www.draytek.com/about/security-advisory/cro	H-DRA-VIRG-290323/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	ss-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2862ln					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2865					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1458
Product: virgor2865ac					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1459
Product: virgor2865ax					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	H-DRA-VIRG-290323/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2865l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2865lac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2865vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: virgor2866					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1464
Product: virgor2866ac					
Affected Version(s): -					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	H-DRA-VIRG-290323/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2866ax					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2866l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2866lac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2866vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1469
Product: virgor2915					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1470
Product: virgor2915ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	H-DRA-VIRG-290323/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2925					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925fn					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1475
Product: virgor2925ln					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1476
Product: virgor2925n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	H-DRA-VIRG-290323/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2925n-plus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925vn-plus					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: virgor2926					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1481
Product: virgor2926ac					
Affected Version(s): -					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	H-DRA-VIRG-290323/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2926l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926lac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926ln					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1486
Product: virgor2926vac					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1487
Product: virgor2927					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	H-DRA-VIRG-290323/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2927ac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927ax					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927f					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927l					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1492
Product: virgor2927lac					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1493
Product: virgor2927vac					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	H-DRA-VIRG-290323/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2952					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2952p					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2962					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: virgor2962p					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1498
Product: virgor3220					
Affected Version(s): -					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	H-DRA-VIRG-290323/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor3910					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	H-DRA-VIRG-290323/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Vendor: heimgardtechnologies					
Product: eagle_1200ac					
Affected Version(s): -					
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepauth_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24117**	N/A	H-HEI-EAGL-290323/1501
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was	N/A	H-HEI-EAGL-290323/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the security parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24118**		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the ssid parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24119**	N/A	H-HEI-EAGL-290323/1503
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wrlEn_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24120**	N/A	H-HEI-EAGL-290323/1504
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the security_5g	N/A	H-HEI-EAGL-290323/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24121**		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the ssid_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24122**	N/A	H-HEI-EAGL-290323/1506
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepauth parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24123**	N/A	H-HEI-EAGL-290323/1507
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wrlEn parameter at /goform/WifiBasicSet.	N/A	H-HEI-EAGL-290323/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24124		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey2_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24125**	N/A	H-HEI-EAGL-290323/1509
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey4_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24126**	N/A	H-HEI-EAGL-290323/1510
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey1 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24127**	N/A	H-HEI-EAGL-290323/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey2 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24128**	N/A	H-HEI-EAGL-290323/1512
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey4 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24129**	N/A	H-HEI-EAGL-290323/1513
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24130**	N/A	H-HEI-EAGL-290323/1514
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was	N/A	H-HEI-EAGL-290323/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the wepkey1_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24131**		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey3_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24132**	N/A	H-HEI-EAGL-290323/1516
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24133**	N/A	H-HEI-EAGL-290323/1517
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the	N/A	H-HEI-EAGL-290323/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wepkey3 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24134**		
Vendor: mediatek					
Product: mt6580					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT65-290323/1519
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT65-290323/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT65-290323/1521
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT65-290323/1522
Time-of-check	07-Mar-2023	6.4	In ion, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT65-290323/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	m/product-security-bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT65-290323/1524
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT65-290323/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Product: mt6731					
Affected Version(s): -					
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1526
Product: mt6735					
Affected Version(s): -					
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1528
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20633		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1530
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1531
Product: mt6737					
Affected Version(s): -					
Time-of-check Time-of-	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to	https://corp.mediatek.com/product-	H-MED-MT67-290323/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	security-bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1533
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Product: mt6739					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1535
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1537
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1538
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT67-290323/1539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	security-bulletin/March-2023	
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1540
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1542
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20623		
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1544
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1545
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1547
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1549
Product: mt6753					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20638		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1551
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1552
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	bulletin/March-2023	
Product: mt6757					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1554
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1556
Product: mt6757c					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1558
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1559
Product: mt6757cd					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1560
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1561
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Product: mt6757ch					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1563
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1565
Product: mt6761					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1567
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1568
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT67-290323/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	security-bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1570
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1572
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20643		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1574
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1575
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1577
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1579
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1581
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1582
Product: mt6762					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	bulletin/March-2023	
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1584
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1586
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1588
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1589
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1591
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1593
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1594
Product: mt6763					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1595
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1596
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1598
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1600
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1602
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1603
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**		
Product: mt6765					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1605
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1607
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1609
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1610
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1612
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1614
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1615
Integer Underflow (Wrap or	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1617
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1619
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20647		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1621
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1622
Product: mt6768					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1623
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1624
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1626
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1628
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1630
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1631
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1633
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1635
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1637
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1638
Product: mt6769					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception.	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1640
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1642
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1644
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1645
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1647
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1649
Product: mt6771					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20621		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1651
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1652
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1654
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1656
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1658
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1659
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1661
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**		
Product: mt6779					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1663
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1665
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1666
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1668
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1670
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1671
Integer Underflow (Wrap or	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1673
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1675
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20647		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1677
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1678
Product: mt6781					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1679
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1680
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1682
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1684
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1686
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1687
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1689
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1691
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1693
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1694
Product: mt6785					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	bulletin/March-2023	
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1696
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1698
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1700
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1701
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1703
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1705
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1707
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1708
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1710
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**		
Product: mt6789					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1712
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20624		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1714
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1715
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-290323/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	bulletin/March-2023	
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1717
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1719
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1721
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1722
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1724
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1726
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT67-290323/1727
Product: mt6833					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1728
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1729
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1731
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**		
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1733
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1735
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1736
Time-of-check Time-of-use (TOCTOU)	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1738
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1740
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1742
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1743
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**		
Product: mt6853					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1745
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1747
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1749
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1750
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1752
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1754
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1755
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race	https://corp.mediatek.com/product-	H-MED-MT68-290323/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	security-bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1757
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1759
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20647		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1761
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1762
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	bulletin/March-2023	
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1764
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1766
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1768
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1769
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	H-MED-MT68-290323/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1771
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1773
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20651		
Product: mt6855					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1775
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1777
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1778
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1780
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1782
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1784
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1785
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1787
Product: mt6873					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1789
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1791
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1792
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1794
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1796
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1797
Time-of-check	07-Mar-2023	6.4	In ion, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT68-290323/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	m/product-security-bulletin/March-2023	
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1799
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1801
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20645		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1803
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1804
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1806
Product: mt6875					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1808
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1810
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1811
Time-of-check	07-Mar-2023	6.4	In ion, there is a possible escalation of	https://corp.mediatek.co	H-MED-MT68-290323/1812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	m/product-security-bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1813
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1815
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20648		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1817
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1818
Product: mt6877					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1819
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1820
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1822
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1824
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1825
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race	https://corp.mediatek.com/product-	H-MED-MT68-290323/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	security-bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1827
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1829
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20646		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1831
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1832
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1834
Product: mt6879					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1836
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1838
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1839
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-290323/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1841
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1843
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20641		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1845
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1846
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1848
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1850
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1852
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1853
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**		
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1855
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	4.1	In adsp, there is a possible escalation of privilege due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07554558;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07554558. **CVE ID : CVE-2023-20620**		
Product: mt6883					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1857
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20624		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1859
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1860
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1862
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1864
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1865
Integer Underflow	07-Mar-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.co	H-MED-MT68-290323/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	m/product-security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1867
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1869
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1871
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1872
Product: mt6885					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1873
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1874
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	bulletin/March-2023	
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1876
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1878
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1880
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1881
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1883
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1885
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1887
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1888
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1890
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**		
Product: mt6889					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1892
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1894
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1895
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1897
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1899
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1901
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1902
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1904
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**		
Product: mt6891					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1906
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1908
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1909
Time-of-check Time-of-use (TOCTOU)	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1911
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1913
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1915
Product: mt6893					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1916
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	bulletin/March-2023	
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1918
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1920
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1922
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1923
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1925
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1927
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1928
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	H-MED-MT68-290323/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1930
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1932
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20649		
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1934
Product: mt6895					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1936
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1937
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**		
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1939
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Improper Input Validation	07-Mar-2023	6.7	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593; Issue ID: ALPS07292593. **CVE ID : CVE-2023-20636**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1941
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1943
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1944
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1946
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**		
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1948
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1949
Integer Underflow (Wrap or	07-Mar-2023	4.4	In keyinstall, there is a possible information	https://corp.mediatek.com/product-	H-MED-MT68-290323/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1951
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1953
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20647		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1955
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1956
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-290323/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	bulletin/March-2023	
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	4.1	In adsp, there is a possible escalation of privilege due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07554558; Issue ID: ALPS07554558. **CVE ID : CVE-2023-20620**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT68-290323/1958
Product: mt6983					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1960
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1962
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1963
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT69-290323/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	security-bulletin/March-2023	
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1965
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1967
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20639		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1969
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1970
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT69-290323/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1972
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1974
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1976
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1977
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1979
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**		
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1981
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	4.1	In adsp, there is a possible escalation of privilege due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07554558; Issue ID: ALPS07554558. **CVE ID : CVE-2023-20620**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1982
Product: mt6985					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593; Issue ID: ALPS07292593. **CVE ID : CVE-2023-20636**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT69-290323/1983
Product: mt8167					
Affected Version(s): -					
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1984
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception.	https://corp.mediatek.com/product-security-	H-MED-MT81-290323/1985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1986
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**		
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1988
Product: mt8167s					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20628		
Product: mt8168					
Affected Version(s): -					
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1990
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1992
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1993
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Improper Input Validation	07-Mar-2023	6.7	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593; Issue ID: ALPS07292593. **CVE ID : CVE-2023-20636**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1995
Product: mt8173					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Product: mt8175					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1997
Product: mt8185					
Affected Version(s): -					
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Product: mt8195z					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT81-290323/1999
Product: mt8321					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20628		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2001
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2002
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-290323/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2004
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2006
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20644		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2008
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2009
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-290323/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2011
Product: mt8362a					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**		
Product: mt8365					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2013
Product: mt8385					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT83-290323/2015
Product: mt8532					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT85-290323/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20623		
Product: mt8666					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2017
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2019
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2020
Time-of-check Time-of-use (TOCTOU)	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2022
Product: mt8667					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2024
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2025
Product: mt8675					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2026
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2027
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT86-290323/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	bulletin/March-2023	
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT86-290323/2029
Product: mt8765					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**		
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2031
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20637		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2033
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2034
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-290323/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2036
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2038
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20646		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2040
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2041
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-290323/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	bulletin/March-2023	
Product: mt8766					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2043
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2045
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2047
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2049
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2050
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2052
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2054
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2055
Product: mt8768					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2056
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2057
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2059
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2061
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2063
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2064
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2066
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2068
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2069
Product: mt8781					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2070
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2071
Improper Input Validation	07-Mar-2023	6.7	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593; Issue ID: ALPS07292593. **CVE ID : CVE-2023-20636**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2073
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2075
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2077
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2078
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2080
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2082
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2084
Product: mt8785					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2085
Product: mt8786					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2086
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2087
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2089
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2091
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2092
Integer Underflow	07-Mar-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.co	H-MED-MT87-290323/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	m/product-security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2094
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2096
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2098
Product: mt8788					
Affected Version(s): -					
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2100
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2101
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2103
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2105
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2106
Integer Underflow (Wrap or	07-Mar-2023	4.4	In keyinstall, there is a possible information	https://corp.mediatek.com/product-	H-MED-MT87-290323/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2108
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2110
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20648		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2112
Product: mt8789					
Affected Version(s): -					
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2114
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2115
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2117
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2119
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2120
Integer Underflow	07-Mar-2023	4.4	In keyinstall, there is a possible	https://corp.mediatek.co	H-MED-MT87-290323/2121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	m/product-security-bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2122
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2124
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2126
Product: mt8791					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530.	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20624		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2128
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2129
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-290323/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**	bulletin/March-2023	
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2131
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2133
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2135
Product: mt8791t					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2136
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception.	https://corp.mediatek.com/product-security-	H-MED-MT87-290323/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2138
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2140
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2142
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2143
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2145
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2147
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2149
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2150
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2152
Product: mt8797					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2154
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2156
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2157
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2159
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2161
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2163
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2164
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2166
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609;	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2168
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2170
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	H-MED-MT87-290323/2171
Vendor: Mitsubishielectric					
Product: fx5-enet					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5--290323/2172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5-enet\/ip					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5--290323/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-30mr\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2174
Product: fx5s-30mt\/es					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5S-290323/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-30mt\/ess					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-40mr\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2177
Product: fx5s-40mt\/es					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5S-290323/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-40mt\/ess					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-60mr\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2180
Product: fx5s-60mt\/es					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5S-290323/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-60mt\/ess					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-80mr\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2183
Product: fx5s-80mt\/es					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5S-290323/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-80mt\/ess					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5S-290323/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uc-32mr\/ds-ts					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2186
Product: fx5uc-32mt\/d					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uc-32mt\/ds-ts					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uc-32mt\/dss					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2189
Product: fx5uc-32mt\/dss-ts					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uc-64mt\/d					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uc-64mt\/dss					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2192
Product: fx5uc-96mt\/d					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uc-96mt\/dss					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-24mr\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2195
Product: fx5uj-24mr\/es-a					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-24mt\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-24mt\/es-a					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2198
Product: fx5uj-24mt\/ess					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-40mr\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-40mr\/es-a					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2201
Product: fx5uj-40mt\/es					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-40mt\/es-a					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-40mt\/ess					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2204
Product: fx5uj-60mr\/es					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-60mr\/es-a					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-60mt\/es					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2207
Product: fx5uj-60mt\/es-a					
Affected Version(s): -					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	H-MIT-FX5U-290323/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-60mt\/ess					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	H-MIT-FX5U-290323/2209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Vendor: Moxa					
Product: uc-2101-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-2-290323/2210
Product: uc-2102-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	H-MOX-UC-2-290323/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2102-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-2-290323/2212
Product: uc-2104-lx					
Affected Version(s): -					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	H-MOX-UC-2-290323/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2111-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-2-290323/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-2112-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-2-290323/2215
Product: uc-2114-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	H-MOX-UC-2-290323/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2116-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-2-290323/2217
Product: uc-3101-t-ap-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	H-MOX-UC-3-290323/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3101-t-eu-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-3-290323/2219
Product: uc-3101-t-us-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	H-MOX-UC-3-290323/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3111-t-ap-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-3-290323/2221
Product: uc-3111-t-ap-lx-nw					
Affected Version(s): -					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	H-MOX-UC-3-290323/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3111-t-eu-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-3-290323/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-3111-t-eu-lx-nw					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-3-290323/2224
Product: uc-3111-t-us-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	H-MOX-UC-3-290323/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3111-t-us-lx-nw					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-3-290323/2226
Product: uc-3121-t-ap-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	H-MOX-UC-3-290323/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3121-t-eu-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-3-290323/2228
Product: uc-3121-t-us-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	H-MOX-UC-3-290323/2229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5101-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-5-290323/2230
Product: uc-5101-t-lx					
Affected Version(s): -					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	H-MOX-UC-5-290323/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5102-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-5-290323/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-5102-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-5-290323/2233
Product: uc-5111-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	H-MOX-UC-5-290323/2234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5111-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-5-290323/2235
Product: uc-5112-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	H-MOX-UC-5-290323/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5112-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-5-290323/2237
Product: uc-8112-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	H-MOX-UC-8-290323/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8112-me-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2239
Product: uc-8112-me-t-lx1					
Affected Version(s): -					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	H-MOX-UC-8-290323/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8112a-me-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-8131-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2242
Product: uc-8132-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	H-MOX-UC-8-290323/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8162-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2244
Product: uc-8210-t-lx-s					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	H-MOX-UC-8-290323/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8220-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2246
Product: uc-8220-t-lx-ap-s					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	H-MOX-UC-8-290323/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8220-t-lx-eu-s					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2248
Product: uc-8220-t-lx-s					
Affected Version(s): -					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	H-MOX-UC-8-290323/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8220-t-lx-us-s					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-8410a-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2251
Product: uc-8410a-nw-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	H-MOX-UC-8-290323/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8410a-nw-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2253
Product: uc-8410a-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	H-MOX-UC-8-290323/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8540-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2255
Product: uc-8540-t-ct-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	H-MOX-UC-8-290323/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8540-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2257
Product: uc-8580-lx					
Affected Version(s): -					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	H-MOX-UC-8-290323/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8580-q-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-8580-t-ct-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2260
Product: uc-8580-t-ct-q-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	H-MOX-UC-8-290323/2261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8580-t-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	H-MOX-UC-8-290323/2262
Product: uc-8580-t-q-lx					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	H-MOX-UC-8-290323/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Vendor: Netgear					
Product: rax30					
Affected Version(s): -					
Improper Authentication	14-Mar-2023	9.8	Netgear RAX30 (AX2400), prior to version 1.0.6.74, was affected by an authentication bypass vulnerability, allowing an unauthenticated attacker to gain administrative access to the device's web management interface by resetting the admin password. **CVE ID : CVE-2023-1327**	N/A	H-NET-RAX3-290323/2264
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a buffer overflow vulnerability in various CGI mechanisms that could allow an attacker to execute arbitrary code on the device.	N/A	H-NET-RAX3-290323/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27852		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a format string vulnerability in a SOAP service that could allow an attacker to execute arbitrary code on the device. **CVE ID : CVE-2023-27853**	N/A	H-NET-RAX3-290323/2266
Cross-Site Request Forgery (CSRF)	10-Mar-2023	8.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 is vulnerable to cross-site request forgery attacks on all endpoints due to improperly implemented CSRF protections. **CVE ID : CVE-2023-1205**	N/A	H-NET-RAX3-290323/2267
N/A	10-Mar-2023	8.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a file sharing mechanism that unintentionally allows users with upload permissions to execute arbitrary code on the device. **CVE ID : CVE-2023-27851**	N/A	H-NET-RAX3-290323/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	15-Mar-2023	8.8	When uploading a firmware image to a Netgear Nighthawk Wifi6 Router (RAX30), a hidden "forceFWUpdate" parameter may be provided to force the upgrade to complete and bypass certain validation checks. End users can use this to upload modified, unofficial, and potentially malicious firmware to the device. **CVE ID : CVE-2023-28337**	N/A	H-NET-RAX3-290323/2269
Allocation of Resources Without Limits or Throttling	15-Mar-2023	7.5	Any request send to a Netgear Nighthawk Wifi6 Router (RAX30)'s web service containing a "Content-Type" of "multipartboundary =" will result in the request body being written to "/tmp/mulipartFile" on the device itself. A sufficiently large file will cause device resources to be exhausted, resulting in the device becoming unusable until it is rebooted. **CVE ID : CVE-2023-28338**	N/A	H-NET-RAX3-290323/2270
N/A	10-Mar-2023	6.8	NETGEAR Nighthawk WiFi6 Router prior to	N/A	H-NET-RAX3-290323/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			V1.0.10.94 contains a file sharing mechanism that allows users with access to this feature to access arbitrary files on the device. **CVE ID : CVE-2023-27850**		
Vendor: poly					
Product: trio_8800					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	5.4	An arbitrary file upload vulnerability in Poly Trio 8800 7.2.2.1094 allows attackers to execute arbitrary code via a crafted ringtone file. **CVE ID : CVE-2023-24282**	N/A	H-POL-TRIO-290323/2272
Vendor: Samsung					
Product: exynos_1080					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24033		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2274
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**		
Product: exynos_1280					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2278
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and	https://semiconductor.samsung.com/support/qua	H-SAM-EXYN-290323/2279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	lity-support/product-security-updates/	
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26074		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when decoding reserved options. **CVE ID : CVE-2023-26076**		
Product: exynos_2200					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2283
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2285
Buffer Copy without Checking Size of Input	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos	https://semiconductor.samsung.com/support/quality-support/pro	H-SAM-EXYN-290323/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	duct-security-updates/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2287
Product: exynos_850					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2288
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**		
Product: exynos_980					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2292
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2294
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980,	https://semiconductor.samsung.com/support/quality-support/product-	H-SAM-EXYN-290323/2295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	security-updates/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2296
Product: exynos_auto_t5123					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2297
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26072		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2299
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2301
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**		
Product: exynos_modem_5123					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2303
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2305
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos	https://semiconductor.samsung.com/support/quality-support/product-	H-SAM-EXYN-290323/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	security-updates/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2307
Buffer Copy without	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile	https://semiconductor.samsung.com/	H-SAM-EXYN-290323/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**	support/quality-support/product-security-updates/	
Product: exynos_modem_5300					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2309
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and	https://semiconductor.samsung.com/support/qua	H-SAM-EXYN-290323/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	lity-support/product-security-updates/	
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26073		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2312
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2314
Product: exynos_w920					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2316
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980,	https://semiconductor.samsung.com/support/quality-support/product-	H-SAM-EXYN-290323/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	security-updates/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-290323/2318
Vendor: sauter-controls					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: modunet300_ey-am300f001					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	H-SAU-MODU-290323/2319
Product: modunet300_ey-am300f002					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in	N/A	H-SAU-MODU-290323/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**		
Product: nova_106_eyk300f001					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	H-SAU-NOVA-290323/2321
Product: nova_220_eyk220f001					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and	N/A	H-SAU-NOVA-290323/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**		
Product: nova_230_eyk230f001					
Affected Version(s): -					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	H-SAU-NOVA-290323/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Sonicwall					
Product: nsa_2600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2324
Product: nsa_2650					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2325
Product: nsa_2700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSA_-290323/2327
Product: nsa_3600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2328
Product: nsa_3650					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2329
Product: nsa_3700					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2330
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSA_-290323/2331
Product: nsa_4600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2332
Product: nsa_4650					
Affected Version(s): -					
Improper Restriction of Excessive	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts	https://psirt.global.sonicwall.com/vuln-	H-SON-NSA_-290323/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	detail/SNWLID-2023-0005	
Product: nsa_4700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2334
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSA_-290323/2335
Product: nsa_5600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**		
Product: nsa_5650					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2337
Product: nsa_5700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2338
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSA_-290323/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0656		
Product: nsa_6600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2340
Product: nsa_6650					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2341
Product: nsa_6700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSA_-290323/2343
Product: nsa_9250					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2344
Product: nsa_9450					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2345
Product: nsa_9650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSA_-290323/2346
Product: nssp12400					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSSP-290323/2347
Product: nssp12800					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSSP-290323/2348
Product: nssp_10700					
Affected Version(s): -					
Improper Restriction of Excessive	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts	https://psirt.global.sonicwall.com/vuln-	H-SON-NSSP-290323/2349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	detail/SNWLID-2023-0005	
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSSP-290323/2350
Product: nssp_11700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSSP-290323/2351
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSSP-290323/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**		
Product: nssp_13700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSSP-290323/2353
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSSP-290323/2354
Product: nssp_15700					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSSP-290323/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1101		
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSSP-290323/2356
Product: nsv_10					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2357
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2358
Product: nsv_100					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2359
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2360
Product: nsv_1600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2361
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-NSV_-290323/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	ID-2023-0004	
Product: nsv_200					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2363
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2364
Product: nsv_25					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-NSV_-290323/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	ID-2023-0005	
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2366
Product: nsv_270					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2367
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0656		
Product: nsv_300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2369
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2370
Product: nsv_400					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2372
Product: nsv_470					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2373
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2374
Product: nsv_50					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2375
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2376
Product: nsv_800					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2377
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-NSV_-290323/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	ID-2023-0004	
Product: nsv_870					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-NSV_-290323/2379
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-NSV_-290323/2380
Product: sm10200					
Affected Version(s): -					
Improper Restriction of Excessive Authentica	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-SM10-290323/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion Attempts			attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	ID-2023-0005	
Product: sm10400					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SM10-290323/2382
Product: sm10800					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SM10-290323/2383
Product: sm9200					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SM92-290323/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1101		
Product: sm9400					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SM94-290323/2385
Product: sm9600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SM96-290323/2386
Product: sm9800					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SM98-290323/2387
Product: sohow					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SOHO-290323/2388
Product: soho_250					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SOHO-290323/2389
Product: soho_250w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-SOHO-290323/2390
Product: tz270					
Affected Version(s): -					
Improper Restriction	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction	https://psirt.global.sonic	H-SON-TZ27-290323/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Excessive Authentication Attempts			of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	wall.com/vuln-detail/SNWLID-2023-0005	
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ27-290323/2392
Product: tz270w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ27-290323/2393
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ27-290323/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**		
Product: tz300					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ30-290323/2395
Product: tz300p					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ30-290323/2396
Product: tz300w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ30-290323/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1101		
Product: tz350					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ35-290323/2398
Product: tz350w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ35-290323/2399
Product: tz370					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ37-290323/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ37-290323/2401
Product: tz370w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ37-290323/2402
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ37-290323/2403
Product: tz400					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ40-290323/2404
Product: tz400w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ40-290323/2405
Product: tz470					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ47-290323/2406
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause	https://psirt.global.sonicwall.com/vuln-detail/SNWL	H-SON-TZ47-290323/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	ID-2023-0004	
Product: tz470w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ47-290323/2408
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ47-290323/2409
Product: tz500					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ50-290323/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**		
Product: tz500w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ50-290323/2411
Product: tz570					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ57-290323/2412
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ57-290323/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0656		
Product: tz570p					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ57-290323/2414
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ57-290323/2415
Product: tz570w					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ57-290323/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ57-290323/2417
Product: tz600					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ60-290323/2418
Product: tz600p					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ60-290323/2419
Product: tz670					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	H-SON-TZ67-290323/2420
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	H-SON-TZ67-290323/2421
Vendor: Tenda					
Product: ax3					
Affected Version(s): -					
Out-of-bounds Write	15-Mar-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the shareSpeed parameter at /goform/WifiGuestSet. **CVE ID : CVE-2023-27239**	N/A	H-TEN-AX3-290323/2422
Improper Neutralization of Special	15-Mar-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a command	N/A	H-TEN-AX3-290323/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			injection vulnerability via the lanip parameter at /goform/AdvSetLanip. **CVE ID : CVE-2023-27240**		
Product: w15e					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the wifiFilterListRemark parameter in the modifyWifiFilterRules function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27061**	N/A	H-TEN-W15E-290323/2424
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the DNSDomainName parameter in the formModifyDnsForward function. This vulnerability allows attackers to cause a Denial of Service	N/A	H-TEN-W15E-290323/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) via a crafted request. **CVE ID : CVE-2023-27063**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	7.5	Tenda V15V1.0 was discovered to contain a buffer overflow vulnerability via the gotoUrl parameter in the formPortalAuth function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27062**	N/A	H-TEN-W15E-290323/2426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	7.5	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the index parameter in the formDelDnsForward function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27064**	N/A	H-TEN-W15E-290323/2427
Buffer Copy without Checking Size of	13-Mar-2023	7.5	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer	N/A	H-TEN-W15E-290323/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			overflow vulnerability via the picName parameter in the formDelWewifiPi function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27065**		
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-Mar-2023	9.8	TOTOlink A7100RU V7.4cu.2313_B20191024 router has a command injection vulnerability. **CVE ID : CVE-2023-25395**	N/A	H-TOT-A710-290323/2429
Vendor: Tp-link					
Product: archer_ax21					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Mar-2023	8.8	TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 contained a command injection vulnerability in the country form of the /cgi-bin/luci;stok=/locale endpoint on the web	N/A	H-TP--ARCH-290323/2430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface. Specifically, the country parameter of the write operation was not sanitized before being used in a call to popen(), allowing an unauthenticated attacker to inject commands, which would be run as root, with a simple POST request. **CVE ID : CVE-2023-1389**		
Operating System					
Vendor: akuvox					
Product: e11_firmware					
Affected Version(s): -					
Use of Hard-coded Credentials	13-Mar-2023	9.8	The Akuvox E11 secure shell (SSH) server is enabled by default and can be accessed by the root user. This password cannot be changed by the user. **CVE ID : CVE-2023-0345**	N/A	O-AKU-E11_-290323/2431
Storing Passwords in a Recoverable Format	13-Mar-2023	9.8	Akuvox E11 uses a weak encryption algorithm for stored passwords and uses a hard-coded password for decryption which could allow the encrypted passwords to be	N/A	O-AKU-E11_-290323/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decrypted from the configuration file. **CVE ID : CVE-2023-0353**		
Missing Authorization	13-Mar-2023	9.1	The Akuvox E11 libvoice library provides unauthenticated access to the camera capture for image and video. This could allow an attacker to view and record image and video from the camera. **CVE ID : CVE-2023-0349**	N/A	O-AKU-E11_-290323/2433
Weak Password Recovery Mechanism for Forgotten Password	13-Mar-2023	9.1	The Akuvox E11 password recovery webpage can be accessed without authentication, and an attacker could download the device key file. An attacker could then use this page to reset the password back to the default. **CVE ID : CVE-2023-0352**	N/A	O-AKU-E11_-290323/2434
Missing Authentication for Critical Function	13-Mar-2023	9.1	The Akuvox E11 web server can be accessed without any user authentication, and this could allow an attacker to access sensitive information, as well as create and download packet	N/A	O-AKU-E11_-290323/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			captures with known default URLs. **CVE ID : CVE-2023-0354**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	13-Mar-2023	8.8	The Akuvox E11 web server backend library allows command injection in the device phone-book contacts functionality. This could allow an attacker to upload files with executable command instructions. **CVE ID : CVE-2023-0351**	N/A	O-AKU-E11_-290323/2436
Improper Authentication	13-Mar-2023	7.5	Akuvox E11 cloud login is performed through an unencrypted HTTP connection. An attacker could gain access to the Akuvox cloud and device if the MAC address of a device if known. **CVE ID : CVE-2023-0346**	N/A	O-AKU-E11_-290323/2437
N/A	13-Mar-2023	7.5	Akuvox E11 allows direct SIP calls. No access control is enforced by the SIP servers, which could allow an attacker to contact any device within Akuvox to call any other device. **CVE ID : CVE-2023-0348**	N/A	O-AKU-E11_-290323/2438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Cryptographic Key	13-Mar-2023	7.5	Akuvox E11 uses a hard-coded cryptographic key, which could allow an attacker to decrypt sensitive information. **CVE ID : CVE-2023-0355**	N/A	O-AKU-E11_-290323/2439
Insufficient Verification of Data Authenticity	13-Mar-2023	6.5	Akuvox E11 does not ensure that a file extension is associated with the file provided. This could allow an attacker to upload a file to the device by changing the extension of a malicious file to an accepted file type. **CVE ID : CVE-2023-0350**	N/A	O-AKU-E11_-290323/2440
N/A	13-Mar-2023	5.3	The Akuvox E11 Media Access Control (MAC) address, a primary identifier, combined with the Akuvox E11 IP address, could allow an attacker to identify the device on the Akuvox cloud. **CVE ID : CVE-2023-0347**	N/A	O-AKU-E11_-290323/2441
Vendor: Apple					
Product: iphone_os					
Affected Version(s): -					
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Navigation in Google	N/A	O-APP-IPHO-290323/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Chrome on iOS prior to 111.0.5563.64 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1225**		
Vendor: apsystems					
Product: energy_communication_unit_firmware					
Affected Version(s): c1.2.5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	14-Mar-2023	9.8	OS command injection affects Altenergy Power Control Software C1.2.5 via shell metacharacters in the index.php/management/set_timezone timezone parameter, because of set_timezone in models/management_model.php. **CVE ID : CVE-2023-28343**	N/A	O-APS-ENER-290323/2443
Vendor: Arubanetworks					
Product: arubaos					
Affected Version(s): From (including) 10.3.0.0 Up to (including) 10.3.1.0					
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22747**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22748**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2445
Improper Neutralization of	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that	https://www.arubanetworks.com/as	O-ARU-ARUB-290323/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22749**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2447

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22750		
Out-of-bounds Write	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22751**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2448
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22752**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22753**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2450
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22754**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22755**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2452
Buffer Copy without Checking Size of Input ('Classic	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22756**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22757**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2454
Improper Neutralization of Special Elements	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-290323/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22758**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22759**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22760**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2457
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system on the device running ArubaOS. **CVE ID : CVE-2023-22761**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2459
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2460
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2462
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2464
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2465
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2467
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22772**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2468
Improper Limitation of a Pathname to a Restricted Directory	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2470
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	A vulnerability exists which allows an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-22775**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2471
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	An authenticated information disclosure vulnerability exists in the ArubaOS web-	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-290323/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based management interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22777**	RUBA-PSA-2023-002.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2473
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	4.8	A vulnerability in the ArubaOS web management interface could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface. **CVE ID : CVE-2023-22778**		
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2475
Affected Version(s): From (including) 8.10.0.0 Up to (including) 8.10.0.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22747**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22748**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2477
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22749**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22750**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2479
Out-of-bounds Write	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22751**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22752**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2481
Buffer Copy without	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in	https://www.arubanetworks.com/as	O-ARU-ARUB-290323/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22753**	sets/alert/ARUBA-PSA-2023-002.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22754**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22755**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2484
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22756**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22757**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2486
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22758**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22759**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2488
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22760**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22761**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2490
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2492
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2493
Improper Neutralization of Special	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-290323/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2495
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22767		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22768**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2497
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2498
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22772**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2500
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2501
Improper Limitation of a Pathname to a Restricted	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**		
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	A vulnerability exists which allows an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-22775**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2503
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	An authenticated information disclosure vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22777**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2504
Improper Limitation of a	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists	https://www.arubanetworks.com/as	O-ARU-ARUB-290323/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	sets/alert/ARUBA-PSA-2023-002.txt	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Mar-2023	4.8	A vulnerability in the ArubaOS web management interface could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-22778**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2506
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**		
Affected Version(s): From (including) 8.6.0.0 Up to (including) 8.6.0.19					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22747**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2508
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22748**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22749**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2510
Improper Neutralization of Special Elements used in a	01-Mar-2023	9.8	There are multiple command injection vulnerabilities that could lead to unauthenticated remote code	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-290323/2511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22750**	RUBA-PSA-2023-002.txt	
Out-of-bounds Write	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22751**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are stack-based buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba Networks access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22752**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2513
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. **CVE ID : CVE-2023-22753**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22754**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22755**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22756**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Mar-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying operating system processes that could lead to unauthenticated remote code execution by sending specially crafted packets via the PAPI	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22757**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22758**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2519
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22759**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22760**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2521
Improper Neutralization of Special Elements used in a	01-Mar-2023	7.2	Authenticated remote command injection vulnerabilities exist in the ArubaOS web-based management	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-290323/2522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS. **CVE ID : CVE-2023-22761**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22762**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2523
Improper Neutralization of Special Elements used in a Command ('Comman	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22763**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22764**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2525
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22765**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2526
Improper Neutralization of Special	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS	https://www.arubanetworks.com/assets/alert/A	O-ARU-ARUB-290323/2527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22766**	RUBA-PSA-2023-002.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22767**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2528
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22768		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22769**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2530
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Mar-2023	7.2	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22770**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2531
Improper Limitation of a Pathname to a Restricted Directory	01-Mar-2023	6.5	An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22772**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22773**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2533
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	6.5	Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22774**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2534
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	A vulnerability exists which allows an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation could allow access to data beyond what is authorized by the users existing privilege level. **CVE ID : CVE-2023-22775**		
Exposure of Resource to Wrong Sphere	01-Mar-2023	6.5	An authenticated information disclosure vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files in the underlying operating system. **CVE ID : CVE-2023-22777**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2536
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Mar-2023	4.9	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-22776**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2537
Improper Neutralization of	01-Mar-2023	4.8	A vulnerability in the ArubaOS web management	https://www.arubanetworks.com/as	O-ARU-ARUB-290323/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			interface could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. **CVE ID : CVE-2023-22778**	sets/alert/ARUBA-PSA-2023-002.txt	
Insufficient Session Expiration	01-Mar-2023	2.4	An insufficient session expiration vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability allows an attacker to keep a session running on an affected device after the removal of the impacted account **CVE ID : CVE-2023-22771**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-002.txt	O-ARU-ARUB-290323/2539
Vendor: baicells					
Product: eg7035-m11_firmware					
Affected Version(s): * Up to (including) bce-odu-1.0.8					
Improper Neutralization of Special Elements used in a	01-Mar-2023	9.8	Baicells EG7035-M11 devices with firmware through BCE-ODU-1.0.8 are vulnerable to improper code	N/A	O-BAI-EG70-290323/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			exploitation via HTTP GET command injections. Commands are executed using pre-login execution and executed with root permissions. The following methods have been tested and validated by a 3rd party analyst and have been confirmed exploitable special thanks to Lionel Musonza for the discovery. **CVE ID : CVE-2023-1097**		
Vendor: Barracuda					
Product: t100b_firmware					
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T100-290323/2541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain shell metacharacters. **CVE ID : CVE-2023-26213**		
Product: t193a_firmware					
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T193-290323/2542
Product: t200c_firmware					
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T200-290323/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**		
Product: t400c_firmware					
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T400-290323/2544
Product: t600d_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T600-290323/2545
Product: t900b_firmware					
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T900-290323/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**		
Product: t93a_firmware					
Affected Version(s): 8.3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Mar-2023	7.2	On Barracuda CloudGen WAN Private Edge Gateway devices before 8 webui-sdwan-1089-8.3.1-174141891, an OS command injection vulnerability exists in /ajax/update_certificate - a crafted HTTP request allows an authenticated attacker to execute arbitrary commands. For example, a name field can contain :password and a password field can contain shell metacharacters. **CVE ID : CVE-2023-26213**	https://campus.barracuda.com/product/cloudgenwan/doc/96024723/release-notes-8-3-1/	O-BAR-T93A-290323/2547
Vendor: bbraun					
Product: battery-pack_sp_with_wifi_firmware					
Affected Version(s): * Up to (including) 053l000092					
Improper Control of Generation	13-Mar-2023	7.2	An improper neutralization of directives in	N/A	O-BBR-BATT-290323/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			dynamically evaluated code vulnerability in the WiFi Battery embedded web server in versions L90/U70 and L92/U92 can be used to gain administrative access to the WiFi communication module. An authenticated user, having access to both the medical device WiFi network (such as a biomedical engineering staff member) and the specific B.Braun Battery Pack SP with WiFi web server credentials, could get administrative (root) access on the infusion pump communication module. This could be used as a vector to start further attacks **CVE ID : CVE-2023-0888**		
Affected Version(s): * Up to (including) 054u000092					
Improper Control of Generation of Code ('Code Injection')	13-Mar-2023	7.2	An improper neutralization of directives in dynamically evaluated code vulnerability in the WiFi Battery embedded web	N/A	O-BBR-BATT-290323/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server in versions L90/U70 and L92/U92 can be used to gain administrative access to the WiFi communication module. An authenticated user, having access to both the medical device WiFi network (such as a biomedical engineering staff member) and the specific B.Braun Battery Pack SP with WiFi web server credentials, could get administrative (root) access on the infusion pump communication module. This could be used as a vector to start further attacks **CVE ID : CVE-2023-0888**		
Vendor: Cisco					
Product: ios_xr					
Affected Version(s): *					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-	O-CIS-IOS_-290323/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	infodisc-9rdOr5Fq	
Affected Version(s): * Up to (excluding) 7.5.3					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	O-CIS-IOS_-290323/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Affected Version(s): * Up to (excluding) 7.6.1					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-	O-CIS-IOS_-290323/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**	load-infodisc-9rdOr5Fq	
Affected Version(s): * Up to (excluding) 7.7.1					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	O-CIS-IOS_-290323/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Affected Version(s): * Up to (excluding) 7.9.1					
Missing Authorization	09-Mar-2023	4.6	A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-load-infodisc-9rdOr5Fq	O-CIS-IOS_-290323/2554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. **CVE ID : CVE-2023-20064**		
Affected Version(s): 7.7					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	O-CIS-IOS_-290323/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Affected Version(s): From (including) 7.6 Up to (excluding) 7.6.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Mar-2023	7.5	A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bfd-XmRescbT	O-CIS-IOS_-290323/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads. **CVE ID : CVE-2023-20049**		
Product: ip_phone_6825_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2558
Product: ip_phone_6841_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2560
Product: ip_phone_6851_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2562
Product: ip_phone_6861_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2564
Product: ip_phone_6871_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2566
Product: ip_phone_7811_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2568
Product: ip_phone_7821_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2570
Product: ip_phone_7832_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2572
Product: ip_phone_7841_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2574
Product: ip_phone_7861_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2576
Product: ip_phone_8811_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2578
Product: ip_phone_8831_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: ip_phone_8832_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2580
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: ip_phone_8841_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2582
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: ip_phone_8845_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2584
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: ip_phone_8851_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2586
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: ip_phone_8861_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2588
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: ip_phone_8865_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	9.8	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20078**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-IP_P-290323/2590
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-IP_P-290323/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	visory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: unified_ip_phone_7945g_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-UNIF-290323/2592
Product: unified_ip_phone_7965g_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based	https://sec.cloudapps.cisco.com/secu	O-CIS-UNIF-290323/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	rity/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	
Product: unified_ip_phone_7975g_firmware					
Affected Version(s): * Up to (excluding) 11.3.7sr1					
Out-of-bounds Write	03-Mar-2023	7.5	Multiple vulnerabilities in the web-based management interface of certain Cisco IP Phones could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20079**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-cmd-inj-KMFynVcP	O-CIS-UNIF-290323/2594
Vendor: Debian					
Product: debian_linux					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.0					
Out-of-bounds Write	01-Mar-2023	7.8	Libde265 v1.0.10 was discovered to contain a heap-buffer-overflow vulnerability in the derive_spatial_luma_vector_prediction function in motion.cc. **CVE ID : CVE-2023-25221**	https://github.com/strukturag/libde265/issues/388	O-DEB-DEBI-290323/2595
NULL Pointer Dereference	01-Mar-2023	6.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the mc_chroma function at motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24751**	https://github.com/strukturag/libde265/issues/379	O-DEB-DEBI-290323/2596
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_hevc_epel_pixels_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24752**	https://github.com/strukturag/libde265/issues/378	O-DEB-DEBI-290323/2597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_weighted_pred_avg_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24754**	https://github.com/strukturag/libde265/issues/382	O-DEB-DEBI-290323/2598
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_weighted_pred_8_fallback function at fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24755**	https://github.com/strukturag/libde265/issues/384	O-DEB-DEBI-290323/2599
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_unweighted_pred_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service	https://github.com/strukturag/libde265/issues/380	O-DEB-DEBI-290323/2600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) via a crafted input file. **CVE ID : CVE-2023-24756**		
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the put_unweighted_pred_16_fallback function at fallback-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24757**	https://github.com/strukturag/libde265/issues/385	O-DEB-DEBI-290323/2601
NULL Pointer Dereference	01-Mar-2023	5.5	libde265 v1.0.10 was discovered to contain a NULL pointer dereference in the ff_hevc_put_weighted_pred_avg_8_sse function at sse-motion.cc. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input file. **CVE ID : CVE-2023-24758**	https://github.com/strukturag/libde265/issues/383	O-DEB-DEBI-290323/2602
Vendor: Dlink					
Product: dir-820l_firmware					
Affected Version(s): 1.06					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Mar-2023	6.5	A heap overflow vulnerability in D-Link DIR820LA1_FW106B02 allows attackers to cause a denial of service via the config.log_to_syslog and log_opt_dropPackets parameters to mydlink_api.ccp. **CVE ID : CVE-2023-25282**	https://www.dlink.com/en/security-bulletin/, https://github.com/migraine-sudo/D_Link_Vuln/tree/main/Permanent%20DDOS%20vulnerability%20in%20emailInfo	O-DLI-DIR--290323/2603
Affected Version(s): 1.06b02					
Out-of-bounds Write	13-Mar-2023	7.5	A stack overflow vulnerability in D-Link DIR820LA1_FW106B02 allows attackers to cause a denial of service via the reserveDHCP_HostName_1.1.1.0 parameter to lan.asp. **CVE ID : CVE-2023-25283**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--290323/2604
Affected Version(s): 105b03					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR820LA1_FW105B03 allows attackers to escalate privileges to root via a crafted payload. **CVE ID : CVE-2023-25279**	https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20In%20tools_AccountName	O-DLI-DIR--290323/2605
Product: dir-867_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.30b07					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-Mar-2023	9.8	OS Command injection vulnerability in D-Link DIR-867 DIR_867_FW1.30B07 allows attackers to execute arbitrary commands via a crafted LocalIPAddress parameter for the SetVirtualServerSettings to HNAP1. **CVE ID : CVE-2023-24762**	N/A	O-DLI-DIR--290323/2606
Vendor: Draytek					
Product: vigor130_firmware					
Affected Version(s): * Up to (excluding) 3.8.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor165_firmware					
Affected Version(s): * Up to (excluding) 4.2.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor166_firmware					
Affected Version(s): * Up to (excluding) 4.2.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2609
Product: vigor2133ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2610
Product: vigor2133fvac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	O-DRA-VIGO-290323/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: vigor2133n_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2133vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2133_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: vigor2135ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2615
Product: vigor2135ax_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	O-DRA-VIGO-290323/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2135fvac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2135vac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2135_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2762ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2620
Product: vigor2762n_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2621
Product: vigor2762vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	O-DRA-VIGO-290323/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2762_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2763ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2763_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2765ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2626
Product: vigor2765ax_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2627
Product: vigor2765va_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	O-DRA-VIGO-290323/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: vigor2765_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2766ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2766ax_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: vigor2766vac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2632
Product: vigor2766_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	O-DRA-VIGO-290323/2633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2832n_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2832_firmware					
Affected Version(s): * Up to (excluding) 3.9.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860ln_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2637
Product: vigor2860l_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2638
Product: vigor2860n-plus_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	O-DRA-VIGO-290323/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: vigor2860n_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860vn-plus_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor2860_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2643
Product: vigor2960_firmware					
Affected Version(s): 1.5.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Mar-2023	7.8	DrayTek Vigor2960 v1.5.1.4 was discovered to contain a command injection vulnerability via the mainfunction.cgi component. **CVE ID : CVE-2023-24229**	N/A	O-DRA-VIGO-290323/2644
Product: vigornic_132_firmware					
Affected Version(s): * Up to (excluding) 3.8.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIGO-290323/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: vigor_2960_firmware					
Affected Version(s): 1.5.1.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Mar-2023	8.8	A vulnerability, which was classified as critical, was found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1225C of the file mainfunction.cgi. The manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-222258 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1162**	N/A	O-DRA-VIGO-290323/2646
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Mar-2023	6.5	A vulnerability has been found in DrayTek Vigor 2960 1.5.1.4 and classified as problematic. Affected by this vulnerability is the function sub_1DA58 of the file mainfunction.cgi. The manipulation leads to path traversal. The attack	N/A	O-DRA-VIGO-290323/2647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222259. **CVE ID : CVE-2023-1163**		
Product: virgor1000b_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2649
Product: virgor2862bn_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2650
Product: virgor2862b_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	O-DRA-VIRG-290323/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2862lac_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862ln_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2862l_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: virgor2862n_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2655
Product: virgor2862vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	O-DRA-VIRG-290323/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2862_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2865ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2865ax_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2865lac_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2660
Product: virgor2865l_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2661
Product: virgor2865vac_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	O-DRA-VIRG-290323/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2865_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2866ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2866ax_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2866lac_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2666
Product: virgor2866l_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2667
Product: virgor2866vac_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	O-DRA-VIRG-290323/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2866_firmware					
Affected Version(s): * Up to (excluding) 4.4.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2915ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2915_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: virgor2925ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2672
Product: virgor2925fn_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	O-DRA-VIRG-290323/2673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2925ln_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925l_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925n-plus_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2925n_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2677
Product: virgor2925vac_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2678
Product: virgor2925vn-plus_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	O-DRA-VIRG-290323/2679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2925_firmware					
Affected Version(s): * Up to (excluding) 3.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926ac_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926lac_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926ln_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2683
Product: virgor2926l_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2684
Product: virgor2926n_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability	O-DRA-VIRG-290323/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	-(cve-2023-23313)/	
Product: virgor2926vac_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2926_firmware					
Affected Version(s): * Up to (excluding) 3.9.9.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927ac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2.	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23313		
Product: virgor2927ax_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2689
Product: virgor2927f_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross	https://www.draytek.com/about/sec	O-DRA-VIRG-290323/2690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	urity-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2927lac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927l_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765,	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927vac_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2927_firmware					
Affected Version(s): * Up to (excluding) 4.4.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2694
Product: virgor2952p_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.9.7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2695
Product: virgor2952_firmware					
Affected Version(s): * Up to (excluding) 3.9.7.4					
Improper Neutralization of Input During Web Page	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and	https://www.draytek.com/about/security-advisory/cross-site-	O-DRA-VIRG-290323/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	scripting-vulnerability-(cve-2023-23313)/	
Product: virgor2962p_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor2962_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor3220_firmware					
Affected Version(s): * Up to (excluding) 3.9.7.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4;	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**		
Product: virgor3910_firmware					
Affected Version(s): * Up to (excluding) 4.3.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2023	6.1	Certain Draytek products are vulnerable to Cross Site Scripting (XSS) via the wlogin.cgi script and user_login.cgi script of the router's web application management portal. This affects Vigor3910, Vigor1000B, Vigor2962 v4.3.2.1; Vigor2865 and Vigor2866 v4.4.1.0; Vigor2927 v4.4.2.2; and Vigor2915, Vigor2765, Vigor2766, Vigor2135 v4.4.2.0; Vigor2763 v4.4.2.1; Vigor2862 and Vigor2926 v3.9.9.0; Vigor2925 v3.9.3; Vigor2952 and Vigor3220 v3.9.7.3; Vigor2133 and Vigor2762 v3.9.6.4; and Vigor2832 v3.9.6.2. **CVE ID : CVE-2023-23313**	https://www.draytek.com/about/security-advisory/cross-site-scripting-vulnerability-(cve-2023-23313)/	O-DRA-VIRG-290323/2700
Vendor: Fedoraproject					
Product: fedora					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 37					
Divide By Zero	01-Mar-2023	7.8	Divide By Zero in GitHub repository vim/vim prior to 9.0.1367. **CVE ID : CVE-2023-1127**	https://github.com/vim/vim/commit/e0f869196930ef5f25a0ac41c9215b09c9ce2d3c, https://huntr.dev/bounties/2d4d309e-4c96-415f-9070-36d0815f1beb	O-FED-FEDO-290323/2701
Vendor: gigamon					
Product: gigavue-os					
Affected Version(s): 5.0.202					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2023	6.1	The help page in GigaVUE-FM, when using GigaVUE-OS software version 5.0 202, does not require an authenticated user. An attacker could enforce a user into inserting malicious JavaScript code into the URI, that could lead to a Reflected Cross site Scripting. **CVE ID : CVE-2023-0746**	https://www.incibe-cert.es/en/early-warning/ics-advisories/xss-vulnerability-gigavue-fm	O-GIG-GIGA-290323/2702
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Autofill in Google	N/A	O-GOO-ANDR-290323/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1223**		
N/A	07-Mar-2023	4.3	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1228**	N/A	O-GOO-ANDR-290323/2704
N/A	07-Mar-2023	4.3	Inappropriate implementation in WebApp Installs in Google Chrome on Android prior to 111.0.5563.64 allowed an attacker who convinced a user to install a malicious WebApp to spoof the contents of the PWA installer via a crafted HTML page. (Chromium security severity: Medium)	N/A	O-GOO-ANDR-290323/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1230		
N/A	07-Mar-2023	4.3	Inappropriate implementation in Autofill in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to potentially spoof the contents of the omnibox via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1231**	N/A	O-GOO-ANDR-290323/2706
N/A	07-Mar-2023	4.3	Inappropriate implementation in Intents in Google Chrome on Android prior to 111.0.5563.64 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1234**	N/A	O-GOO-ANDR-290323/2707
Affected Version(s): 10.0					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**		
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2709
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778.	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20623		
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2711
Affected Version(s): 11.0					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2712
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	O-GOO-ANDR-290323/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**	security-bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2714
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**		
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2716
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697.	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20634		
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2718
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2719
Affected Version(s): 12.0					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-GOO-ANDR-290323/2720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	bulletin/March-2023	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530. **CVE ID : CVE-2023-20624**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2721
Improper Input Validation	07-Mar-2023	6.7	In msdc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07405223; Issue ID: ALPS07405223. **CVE ID : CVE-2023-20626**		
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2723
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2725
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2726
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Out-of-bounds Write	07-Mar-2023	6.7	In widevine, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07635697; Issue ID: ALPS07635697. **CVE ID : CVE-2023-20634**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2728
Improper Input Validation	07-Mar-2023	6.7	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593;	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07292593. **CVE ID : CVE-2023-20636**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2730
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2732
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2733
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586; Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2735
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584;	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**		
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2737
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2738
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race	https://corp.mediatek.com/product-	O-GOO-ANDR-290323/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	security-bulletin/March-2023	
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2740
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2742
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536; Issue ID: ALPS07628536.	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20646		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2744
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2745
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	O-GOO-ANDR-290323/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	bulletin/March-2023	
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2747
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	4.1	In adsp, there is a possible escalation of privilege due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07554558; Issue ID: ALPS07554558. **CVE ID : CVE-2023-20620**		
Affected Version(s): 13.0					
Improper Input Validation	07-Mar-2023	6.7	In tinysys, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664755; Issue ID: ALPS07664755. **CVE ID : CVE-2023-20621**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2749
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Mar-2023	6.7	In vow, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628530; Issue ID: ALPS07628530.	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20624		
Incorrect Calculation of Buffer Size	07-Mar-2023	6.7	In pqframework, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629585; Issue ID: ALPS07629585. **CVE ID : CVE-2023-20627**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2751
N/A	07-Mar-2023	6.7	In thermal, there is a possible memory corruption due to an uncaught exception. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07494460; Issue ID: ALPS07494460. **CVE ID : CVE-2023-20628**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2752
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	O-GOO-ANDR-290323/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628505; Issue ID: ALPS07628505. **CVE ID : CVE-2023-20630**	bulletin/March-2023	
Out-of-bounds Write	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628506; Issue ID: ALPS07628506. **CVE ID : CVE-2023-20632**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2754
Improper Validation of Array Index	07-Mar-2023	6.7	In usb, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628508; Issue ID: ALPS07628508. **CVE ID : CVE-2023-20633**		
Improper Input Validation	07-Mar-2023	6.7	In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07292593; Issue ID: ALPS07292593. **CVE ID : CVE-2023-20636**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2756
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628588; Issue ID: ALPS07628588. **CVE ID : CVE-2023-20637**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628537; Issue ID: ALPS07628537. **CVE ID : CVE-2023-20638**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2758
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628587; Issue ID: ALPS07628587. **CVE ID : CVE-2023-20639**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2759
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629573; Issue ID: ALPS07629573. **CVE ID : CVE-2023-20640**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629574; Issue ID: ALPS07629574. **CVE ID : CVE-2023-20641**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2761
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628586;	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628586. **CVE ID : CVE-2023-20642**		
Improper Input Validation	07-Mar-2023	6.7	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628584; Issue ID: ALPS07628584. **CVE ID : CVE-2023-20643**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2763
Improper Input Validation	07-Mar-2023	6.7	In apu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629577; Issue ID: ALPS07629577. **CVE ID : CVE-2023-20650**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization	07-Mar-2023	6.4	In adsp, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628532; Issue ID: ALPS07628532. **CVE ID : CVE-2023-20625**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2765
Integer Underflow (Wrap or Wraparound)	07-Mar-2023	4.4	In keyinstall, there is a possible information disclosure due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07563028; Issue ID: ALPS07563028. **CVE ID : CVE-2023-20635**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2766
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628603; Issue ID: ALPS07628603. **CVE ID : CVE-2023-20644**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628609; Issue ID: ALPS07628609. **CVE ID : CVE-2023-20645**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2768
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628536;	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628536. **CVE ID : CVE-2023-20646**		
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628547; Issue ID: ALPS07628547. **CVE ID : CVE-2023-20647**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2770
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628612; Issue ID: ALPS07628612. **CVE ID : CVE-2023-20648**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Mar-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628607; Issue ID: ALPS07628607. **CVE ID : CVE-2023-20649**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2772
Improper Input Validation	07-Mar-2023	4.4	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629576; Issue ID: ALPS07629576. **CVE ID : CVE-2023-20651**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2773
Time-of-check Time-of-use (TOCTOU)	07-Mar-2023	4.1	In adsp, there is a possible escalation of privilege due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/March-2023	O-GOO-ANDR-290323/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07554558; Issue ID: ALPS07554558. **CVE ID : CVE-2023-20620**		
Product: linux_and_chrome_os					
Affected Version(s): -					
Use After Free	07-Mar-2023	8.8	Use after free in Core in Google Chrome on Lacros prior to 111.0.5563.64 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2023-1227**	N/A	O-GOO-LINU-290323/2775
Vendor: heimgardtechnologies					
Product: eagle_1200ac_firmware					
Affected Version(s): 15.03.06.33					
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepauth_5g parameter at	N/A	O-HEI-EAGL-290323/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/goform/WifiBasicSet. **CVE ID : CVE-2023-24117**		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the security parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24118**	N/A	O-HEI-EAGL-290323/2777
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the ssid parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24119**	N/A	O-HEI-EAGL-290323/2778
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wrlEn_5g parameter at /goform/WifiBasicSet.	N/A	O-HEI-EAGL-290323/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24120		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the security_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24121**	N/A	O-HEI-EAGL-290323/2780
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the ssid_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24122**	N/A	O-HEI-EAGL-290323/2781
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepauth parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24123**	N/A	O-HEI-EAGL-290323/2782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wrlEn parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24124**	N/A	O-HEI-EAGL-290323/2783
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey2_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24125**	N/A	O-HEI-EAGL-290323/2784
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey4_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24126**	N/A	O-HEI-EAGL-290323/2785
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was	N/A	O-HEI-EAGL-290323/2786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered to contain a stack overflow via the wepkey1 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24127**		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey2 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24128**	N/A	O-HEI-EAGL-290323/2787
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey4 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24129**	N/A	O-HEI-EAGL-290323/2788
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the	N/A	O-HEI-EAGL-290323/2789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wepkey parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24130**		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey1_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24131**	N/A	O-HEI-EAGL-290323/2790
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey3_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24132**	N/A	O-HEI-EAGL-290323/2791
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey_5g parameter at /goform/WifiBasicSet.	N/A	O-HEI-EAGL-290323/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24133		
Out-of-bounds Write	01-Mar-2023	6.5	Jensen of Scandinavia Eagle 1200AC V15.03.06.33_en was discovered to contain a stack overflow via the wepkey3 parameter at /goform/WifiBasicSet. **CVE ID : CVE-2023-24134**	N/A	O-HEI-EAGL-290323/2793
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	https://www.ibm.com/support/pages/node/6958522, https://exchange.xforce.ibmcloud.com/vulnerabilities/248296	O-HP-HP-U-290323/2794
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service	https://www.ibm.com/support/pages/node/6958522, https://exchange.xforce.i	O-IBM-AIX-290323/2795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	bmcloud.com/vulnerabilities/248296	
Product: z\/os					
Affected Version(s): -					
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	https://www.ibm.com/support/pages/node/6958522, https://exchange.xforce.ibmcloud.com/vulnerabilities/248296	O-IBM-Z\/O-290323/2796
Vendor: kylinos					
Product: kylin_os					
Affected Version(s): * Up to (excluding) 1.3.11-23					
Incorrect Authorization	03-Mar-2023	7.8	A vulnerability was found in KylinSoft kylin-activation and classified as critical. Affected by this issue is some unknown functionality of the component File Import. The manipulation leads to improper authorization. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.11-23	N/A	O-KYL-KYLI-290323/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 1.30.10-5.p23 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222260. **CVE ID : CVE-2023-1164**		
Affected Version(s): * Up to (excluding) 1.30.10-5.p23					
Incorrect Authorization	03-Mar-2023	7.8	A vulnerability was found in KylinSoft kylin-activation and classified as critical. Affected by this issue is some unknown functionality of the component File Import. The manipulation leads to improper authorization. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.11-23 and 1.30.10-5.p23 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-222260. **CVE ID : CVE-2023-1164**	N/A	O-KYL-KYLI-290323/2798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	https://www.ibm.com/support/pages/node/6958522, https://exchange.xforce.ibmcloud.com/vulnerabilities/248296	O-LIN-LINU-290323/2799
Affected Version(s): * Up to (excluding) 5.0					
Use After Free	08-Mar-2023	7.8	A use-after-free flaw was found in the Linux kernel's nouveau driver in how a user triggers a memory overflow that causes the nvkm_vma_tail function to fail. This flaw allows a local user to crash or potentially escalate their privileges on the system. **CVE ID : CVE-2023-0030**	https://github.com/torvalds/linux/commit/729eba3355674f2d9524629b73683ba1d1cd3f10, https://bugzilla.redhat.com/show_bug.cgi?id=2157270	O-LIN-LINU-290323/2800
Affected Version(s): * Up to (excluding) 5.15.13					
NULL Pointer Dereference	01-Mar-2023	5.5	In the Linux kernel before 5.15.13, drivers/net/ethernet/mellanox/mlx5/core/steering/dr_domain.c misinterprets the mlx5_get_uars_page return value (expects	https://github.com/torvalds/linux/commit/6b8b42585886c59a008015083282aae434349094,	O-LIN-LINU-290323/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			it to be NULL in the error case, whereas it is actually an error pointer). **CVE ID : CVE-2023-23006**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.13	
Affected Version(s): * Up to (excluding) 5.16					
Unchecked Return Value	01-Mar-2023	7.8	In the Linux kernel before 5.16, tools/perf/util/expr.c lacks a check for the hashmap_new return value. **CVE ID : CVE-2023-23003**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16, https://github.com/torvalds/linux/commit/0a515a06c5ebfa46fee3ac519e418f801e718da4	O-LIN-LINU-290323/2802
Affected Version(s): * Up to (excluding) 5.16.3					
NULL Pointer Dereference	01-Mar-2023	5.5	In the Linux kernel before 5.16.3, drivers/scsi/ufs/ufs-mediatek.c misinterprets the regulator_get return value (expects it to be NULL in the error case, whereas it is actually an error pointer). **CVE ID : CVE-2023-23001**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.3, https://github.com/torvalds/linux/commit/3ba880a12df5aa4488c18281701b5b1bc3d4531a	O-LIN-LINU-290323/2803
NULL Pointer Dereference	01-Mar-2023	5.5	In the Linux kernel before 5.16.3, drivers/bluetooth/hci_qca.c misinterprets the devm_gpiod_get_index_optional return	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.16.3, https://githu	O-LIN-LINU-290323/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value (expects it to be NULL in the error case, whereas it is actually an error pointer). **CVE ID : CVE-2023-23002**	b.com/torvalds/linux/commit/6845667146a28c09b5dfc401c1ad112374087944	
Affected Version(s): * Up to (excluding) 5.17					
NULL Pointer Dereference	01-Mar-2023	7.8	In the Linux kernel before 5.17, drivers/phy/tegra/xusb.c mishandles the tegra_xusb_find_port_node return value. Callers expect NULL in the error case, but an error pointer is used. **CVE ID : CVE-2023-23000**	https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.17, https://github.com/torvalds/linux/commit/045a31b95509c8f25f5f04ec5e0dec5cd09f2c5f	O-LIN-LINU-290323/2805
Affected Version(s): * Up to (excluding) 5.19					
NULL Pointer Dereference	01-Mar-2023	5.5	In the Linux kernel before 5.19, drivers/gpu/drm/arm/malidp_planes.c misinterprets the get_sg_table return value (expects it to be NULL in the error case, whereas it is actually an error pointer). **CVE ID : CVE-2023-23004**	https://github.com/torvalds/linux/commit/15342f930ebebcfe36f2415049736a77d7d2e045, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19	O-LIN-LINU-290323/2806
Affected Version(s): * Up to (excluding) 6.2					
NULL Pointer Dereference	01-Mar-2023	5.5	** DISPUTED ** In the Linux kernel before 6.2, mm/memory-tiers.c misinterprets the	https://github.com/torvalds/linux/commit/4a625ceee8a0ab02	O-LIN-LINU-290323/2807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			alloc_memory_type return value (expects it to be NULL in the error case, whereas it is actually an error pointer). NOTE: this is disputed by third parties because there are no realistic cases in which a user can cause the alloc_memory_type error case to be reached. **CVE ID : CVE-2023-23005**	73534cb6b432ce6b331db5ee, https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.2, https://bugzilla.suse.com/show_bug.cgi?id=1208844#c2	
Affected Version(s): * Up to (excluding) 6.3					
Use After Free	02-Mar-2023	7.8	A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user detaching rc device. A local user could use this flaw to crash the system or potentially escalate their privileges on the system. **CVE ID : CVE-2023-1118**	https://github.com/torvalds/linux/commit/29b0589a865b6f66d141d79b2dd1373e4e50fe17	O-LIN-LINU-290323/2808
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Uncontrolled Search Path Element	10-Mar-2023	9.8	An uncontrolled search path element vulnerability in the Trend Micro Apex One Server installer could allow an	https://success.trendmicro.com/solution/000292209	O-MIC-WIND-290323/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to achieve a remote code execution state on affected products. **CVE ID : CVE-2023-25143**		
N/A	10-Mar-2023	7.8	An improper access control vulnerability in the Trend Micro Apex One agent could allow a local attacker to gain elevated privileges and create arbitrary directories with arbitrary ownership. **CVE ID : CVE-2023-25144**	https://success.trendmicro.com/solution/000292209	O-MIC-WIND-290323/2810
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A link following vulnerability in the scanning function of Trend Micro Apex One agent 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-2023-25145**	https://success.trendmicro.com/solution/000292209	O-MIC-WIND-290323/2811
Improper Link Resolution Before File Access	10-Mar-2023	7.8	A security agent link following vulnerability in the Trend Micro Apex One agent could allow a local attacker	https://success.trendmicro.com/solution/000292209	O-MIC-WIND-290323/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			to quarantine a file, delete the original folder and replace with a junction to an arbitrary location, ultimately leading to an arbitrary file dropped to an arbitrary location. 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-2023-25146**		
Improper Link Resolution Before File Access ('Link Following')	10-Mar-2023	7.8	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to exploit the vulnerability by changing a specific file into a pseudo-symlink, allowing privilege escalation 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-2023-25148**	https://success.trendmicro.com/solution/000292209	O-MIC-WIND-290323/2813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	https://www.ibm.com/support/pages/node/6958522, https://exchange.xforce.ibmcloud.com/vulnerabilities/248296	O-MIC-WIND-290323/2814
Uncontrolled Search Path Element	10-Mar-2023	6.7	An issue in the Trend Micro Apex One agent could allow an attacker who has previously acquired administrative rights via other means to bypass the protection by using a specifically crafted DLL during a specific update process. Please note: an attacker must first obtain administrative access on the target system via another method in order to exploit this. **CVE ID : CVE-2023-25147**	https://success.trendmicro.com/solution/000292209	O-MIC-WIND-290323/2815
Out-of-bounds Write	07-Mar-2023	6.5	Stack buffer overflow in Crash reporting in Google Chrome on Windows prior to 111.0.5563.64 allowed a remote attacker who had compromised the	N/A	O-MIC-WIND-290323/2816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1217**		
NULL Pointer Dereference	06-Mar-2023	5.5	A vulnerability has been found in FabulaTech Webcam for Remote Desktop 2.8.42 and classified as problematic. This vulnerability affects unknown code in the library ftwebcam.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. VDB-222358 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1186**	N/A	O-MIC-WIND-290323/2817
Improper Resource Shutdown or Release	06-Mar-2023	5.5	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42 and classified as problematic. This issue affects some	N/A	O-MIC-WIND-290323/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown processing in the library ftwebcam.sys of the component Global Variable Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-222359. **CVE ID : CVE-2023-1187**		
Improper Resource Shutdown or Release	06-Mar-2023	5.5	A vulnerability was found in FabulaTech Webcam for Remote Desktop 2.8.42. It has been classified as problematic. Affected is an unknown function in the library ftwebcam.sys of the component IoControlCode Handler. The manipulation leads to denial of service. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-222360.	N/A	O-MIC-WIND-290323/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1188		
Out-of-bounds Read	10-Mar-2023	4.4	NVIDIA CUDA Toolkit SDK contains a vulnerability in cuobjdump, where a local user running the tool against a malicious binary may cause an out-of-bounds read, which may result in a limited denial of service and limited information disclosure. **CVE ID : CVE-2023-0193**	https://nvidia.custhelp.com/app/answers/detail/a_id/5446	O-MIC-WIND-290323/2820
NULL Pointer Dereference	02-Mar-2023	3.3	NVIDIA CUDA Toolkit SDK contains a bug in cuobjdump, where a local user running the tool against an ill-formed binary may cause a null- pointer dereference, which may result in a limited denial of service. **CVE ID : CVE-2023-0196**	https://nvidia.custhelp.com/app/answers/detail/a_id/5446	O-MIC-WIND-290323/2821
Product: windows_10					
Affected Version(s): * Up to (excluding) 10.0.10240.19805					
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/2822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/2823
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/2824
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/2825
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/2826
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/2827
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24858		
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/2829
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.19805					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/2830
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/2831
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/2832
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24907		
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/2834
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/2835
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/2836
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/2837
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 10.0.10240.19805					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/2839
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/2840
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/2841
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/2842
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/2843
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-290323/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	m/update-guide/vulnerability/CVE-2023-24872	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/2845
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/2846
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/2847
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/2848
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23401	ability/CVE-2023-23401	
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/2850
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/2851
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/2852
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/2853
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/2854
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE)	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	guide/vulnerability/CVE-2023-23414	
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/2856
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/2857
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/2858
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/2859
Exposure of Resource	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Disclosure Vulnerability **CVE ID : CVE-2023-23394**	ability/CVE-2023-23394	
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/2861
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/2862
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.5786					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/2863
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/2864
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24868		
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/2866
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/2867
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/2868
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/2869
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/2870

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/2871
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/2872
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/2873
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/2874
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/2875
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/2876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/2877
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/2878
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/2879
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/2880
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/2881
Exposure of Resource	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/2882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	guide/vulnerability/CVE-2023-24906	
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/2883
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/2884
Affected Version(s): 10.0.14393.5786					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/2885
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/2886
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/2888
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/2889
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/2890
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/2891
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/2893
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/2894
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/2895
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/2896
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/2897
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/2898

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/2899
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/2900
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/2901
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/2902
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/2903
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE)	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/2904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	guide/vulnerability/CVE-2023-23385	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/2905
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/2906
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/2907
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/2908
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23409	ability/CVE-2023-23409	
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/2910
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.4131					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/2911
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/2912
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/2913
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24907		
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/2915
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/2916
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/2917
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/2918
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/2919
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23422	ability/CVE-2023-23422	
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/2921
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/2922
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/2923
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/2924
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/2925
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE)	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/2926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	guide/vulnerability/CVE-2023-24859	
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/2927
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/2928
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/2929
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/2930
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24911**	ability/CVE-2023-24911	
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/2932
Affected Version(s): 10.0.17763.4131					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/2933
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/2934
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/2935
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/2936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/2937
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/2938
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/2939
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/2940
Concurrent Execution using Shared Resource with Improper Synchronization	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/2942
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/2943
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/2944
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/2945
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/2946
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/2947
N/A	14-Mar-2023	7.8	Windows Cryptographic	https://msrc.microsoft.co	O-MIC-WIND-290323/2948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	m/update-guide/vulnerability/CVE-2023-23416	
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/2949
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/2950
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/2951
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/2952
Concurrent Execution using Shared	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Privilege Vulnerability **CVE ID : CVE-2023-23393**	ability/CVE-2023-23393	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/2954
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/2955
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/2956
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/2957
Exposure of Resource	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/2958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Disclosure Vulnerability **CVE ID : CVE-2023-23409**	guide/vulnerability/CVE-2023-23409	
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/2959
Product: windows_10_20h2					
Affected Version(s): * Up to (excluding) 10.0.19042.2728					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/2960
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/2961
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/2962
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24907**	ability/CVE-2023-24907	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/2964
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/2965
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/2966
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/2967
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/2969
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/2970
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/2971
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/2972
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/2973
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/2974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24858		
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/2975
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/2976
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/2977
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/2978
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/2979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/2980
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/2981
Affected Version(s): 10.0.19042.2728					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/2982
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/2983
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/2984
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23403		
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/2986
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/2987
N/A	14-Mar-2023	8.8	Windows Bluetooth Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-24871**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24871	O-MIC-WIND-290323/2988
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/2989
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/2990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/2991
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/2992
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/2993
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/2994
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/2995
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/2996

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/2997
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/2998
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/2999
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3000
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3001
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE)	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	guide/vulnerability/CVE-2023-23385	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3003
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3004
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3005
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3007
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3008
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3009
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.2728					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3010
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3011
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	guide/vulnerability/CVE-2023-24868	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3013
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3014
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3015
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3016
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ability/CVE-2023-23420	
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3018
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3019
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3020
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3021
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3022
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24857		
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3024
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3025
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3026
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3027
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3029
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3030
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3031
Affected Version(s): 10.0.19044.2728					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3032
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3033
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23388	ability/CVE-2023-23388	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3035
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3036
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3037
N/A	14-Mar-2023	8.8	Windows Bluetooth Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-24871**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24871	O-MIC-WIND-290323/3038
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3040
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3041
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3042
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3043
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3044
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23402	ability/CVE-2023-23402	
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3046
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3047
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3048
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/3049
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3050
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE)	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	guide/vulnerability/CVE-2023-23414	
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3052
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3053
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3054
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3056
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3057
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3058
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3059
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.2728					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3060
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	guide/vulnerability/CVE-2023-24867	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3062
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3063
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3064
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3065
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-24908**	ability/CVE-2023-24908	
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3067
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3068
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3069
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3070
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3071
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24856		
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3073
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3074
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3075
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3076
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3078
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3079
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3080
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3081
Affected Version(s): 10.0.19045.2728					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3082
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-23415**	guide/vulnerability/CVE-2023-23415	
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/3084
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3085
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3086
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3087
N/A	14-Mar-2023	8.8	Windows Bluetooth Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-24871**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24871	O-MIC-WIND-290323/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3089
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3090
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3091
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3092
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3093
N/A	14-Mar-2023	7.8	Windows Media Remote Code	https://msrc.microsoft.co	O-MIC-WIND-290323/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-23401**	m/update-guide/vulnerability/CVE-2023-23401	
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3095
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3096
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3097
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3098
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/3099
Concurrent Execution using Shared Resource	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Execution Vulnerability **CVE ID : CVE-2023-23407**	ability/CVE-2023-23407	
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3101
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3102
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3103
Concurrent Execution using Shared Resource with Improper Synchronization	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3105
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3106
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3107
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3108
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3109
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.1696					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-290323/3110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	m/update-guide/vulnerability/CVE-2023-24864	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3111
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3112
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3113
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3114
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24913**	ability/CVE-2023-24913	
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3116
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3117
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3118
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3119
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3120
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3122
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3123
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3124
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3125
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3126
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	guide/vulnerability/CVE-2023-24865	
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3128
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3129
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3130
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3131
Affected Version(s): 10.0.22000.1696					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21708	ability/CVE-2023-21708	
N/A	14-Mar-2023	9.8	HTTP Protocol Stack Remote Code Execution Vulnerability **CVE ID : CVE-2023-23392**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392	O-MIC-WIND-290323/3133
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3134
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/3135
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3136
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3137
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	guide/vulnerability/CVE-2023-23413	
N/A	14-Mar-2023	8.8	Windows Bluetooth Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-24871**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24871	O-MIC-WIND-290323/3139
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3140
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3141
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3142
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-23405**	guide/vulnerability/CVE-2023-23405	
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3144
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3145
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3146
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3147
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3148
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23417	ability/CVE-2023-23417	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3150
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3151
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3152
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3153
Concurrent Execution using	14-Mar-2023	7	Windows Graphics Component	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	guide/vulnerability/CVE-2023-24861	
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3155
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3156
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3157
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3158
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ability/CVE-2023-24862	
Product: windows_11_22h2					
Affected Version(s): -					
N/A	14-Mar-2023	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23418**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23418	O-MIC-WIND-290323/3160
Affected Version(s): * Up to (excluding) 10.0.22000.1413					
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3161
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3162
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3163
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24907		
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3165
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3166
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3167
N/A	14-Mar-2023	7.8	Windows Resilient File System (ReFS) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23419**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23419	O-MIC-WIND-290323/3168
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3169
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23421	ability/CVE-2023-23421	
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3171
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3172
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3173
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3174
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3175
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24858**	ability/CVE-2023-24858	
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3177
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3178
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3179
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3180
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24906		
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3182
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3183
Affected Version(s): 10.0.22000.1413					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3184
N/A	14-Mar-2023	9.8	HTTP Protocol Stack Remote Code Execution Vulnerability **CVE ID : CVE-2023-23392**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392	O-MIC-WIND-290323/3185
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3186
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23388	ability/CVE-2023-23388	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3188
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3189
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3190
N/A	14-Mar-2023	8.8	Windows Bluetooth Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-24871**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24871	O-MIC-WIND-290323/3191
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3193
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3194
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3195
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3196
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3197
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23402	ability/CVE-2023-23402	
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3199
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3200
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/3201
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3202
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3204
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3205
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3206
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3207
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24870		
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3209
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3210
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3211
Product: windows_server_2008					
Affected Version(s): -					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3212
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3213
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-23405**	guide/vulnerability/CVE-2023-23405	
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3215
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3216
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3217
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3218
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3219
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3221
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3222
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3223
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3224
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3225
Concurrent Execution using Shared Resource with Improper Synchronization	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3227
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3228
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3229
Affected Version(s): r2					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3230
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3231
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23405	ability/CVE-2023-23405	
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3233
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3234
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3235
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3236
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3237
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3239
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3240
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3241
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3242
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3243
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23414		
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3245
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3246
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3247
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3248
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3249
Product: windows_server_2012					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3250
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3251
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3252
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3253
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3254
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-290323/3255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	m/update-guide/vulnerability/CVE-2023-24872	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3256
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3257
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3258
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3259
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	guide/vulnerability/CVE-2023-24909	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3261
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3262
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3263
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3264
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24869	ability/CVE-2023-24869	
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3266
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3267
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3268
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3269
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3270
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3272
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3273
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3274
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3275
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3276
Concurrent Execution using Shared Resource	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Execution Vulnerability **CVE ID : CVE-2023-23407**	ability/CVE-2023-23407	
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3278
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3279
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3280
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3282
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3283
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3284
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3285
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3287
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3288
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3289
Affected Version(s): r2					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3290
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3291
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24876**	ability/CVE-2023-24876	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3293
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3294
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3295
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3296
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-23403**	ability/CVE-2023-23403	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3298
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3299
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3300
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3301
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24909**	ability/CVE-2023-24909	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3303
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3304
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3305
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3306
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3308
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3309
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3310
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3311
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3312
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3313
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ability/CVE-2023-23410	
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3315
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3316
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3317
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3318
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3319
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE)	https://msrc.microsoft.co	O-MIC-WIND-290323/3320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	m/update-guide/vulnerability/CVE-2023-24859	
N/A	14-Mar-2023	7.2	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-23400**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400	O-MIC-WIND-290323/3321
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3322
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3323
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3324
Concurrent Execution using Shared Resource	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2023-24861**	ability/CVE-2023-24861	
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3326
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3327
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3328
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3329
Exposure of Resource	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	guide/vulnerability/CVE-2023-24906	
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3331
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3332
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3333
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3334
Product: windows_server_2016					
Affected Version(s): -					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21708	ability/CVE-2023-21708	
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3336
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3337
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/3338
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3339
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3341
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3342
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3343
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3344
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3346
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3347
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3348
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3349
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3351
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3352
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3353
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3354
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/3355
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3356
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23421	guide/vulnerability/CVE-2023-23421	
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3358
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3359
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3360
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3361
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3362
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3364
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3365
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3366
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3367
N/A	14-Mar-2023	7.2	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-23400**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400	O-MIC-WIND-290323/3368
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-23414**	ability/CVE-2023-23414	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3370
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3371
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3372
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3374
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3375
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3376
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3377
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3378
Uncontrolled Resource	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-290323/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			**CVE ID : CVE-2023-24862**	guide/vulnerability/CVE-2023-24862	
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3380
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3381
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3382
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3383
Product: windows_server_2019					
Affected Version(s): -					
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3384

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3385
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/3386
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3387
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24876**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3388
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3389
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24913**	ability/CVE-2023-24913	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3391
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3392
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3393
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3394
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	ability/CVE-2023-24864	
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3396
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3397
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3398
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3399
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23405	ability/CVE-2023-23405	
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3401
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3402
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3403
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3404
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/3405
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3407
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3408
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3409
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3410
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23402**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3411
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3412
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24859	ability/CVE-2023-24859	
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3414
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3415
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3416
N/A	14-Mar-2023	7.2	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-23400**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400	O-MIC-WIND-290323/3417
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3419
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3420
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3421
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3422
Exposure of	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class	https://msrc.microsoft.co	O-MIC-WIND-290323/3423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	m/update-guide/vulnerability/CVE-2023-24863	
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3424
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24866**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24866	O-MIC-WIND-290323/3425
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3426
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3427
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24906**	ability/CVE-2023-24906	
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3429
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3430
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3431
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3432
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3433
Product: windows_server_2022					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	9.8	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-21708**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708	O-MIC-WIND-290323/3434
N/A	14-Mar-2023	9.8	HTTP Protocol Stack Remote Code Execution Vulnerability **CVE ID : CVE-2023-23392**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392	O-MIC-WIND-290323/3435
N/A	14-Mar-2023	9.8	Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23415**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415	O-MIC-WIND-290323/3436
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24907**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24907	O-MIC-WIND-290323/3437
N/A	14-Mar-2023	8.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23388**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23388	O-MIC-WIND-290323/3438
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24876	O-MIC-WIND-290323/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24876		
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23413**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23413	O-MIC-WIND-290323/3440
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23406**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23406	O-MIC-WIND-290323/3441
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24872**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24872	O-MIC-WIND-290323/3442
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-23403**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23403	O-MIC-WIND-290323/3443
N/A	14-Mar-2023	8.8	Windows Bluetooth Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-24871**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24871	O-MIC-WIND-290323/3444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24913**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24913	O-MIC-WIND-290323/3445
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24868**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24868	O-MIC-WIND-290323/3446
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24867**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24867	O-MIC-WIND-290323/3447
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24864**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24864	O-MIC-WIND-290323/3448
N/A	14-Mar-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24909**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24909	O-MIC-WIND-290323/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24869**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869	O-MIC-WIND-290323/3450
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	8.1	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-23404**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23404	O-MIC-WIND-290323/3451
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-23405**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405	O-MIC-WIND-290323/3452
N/A	14-Mar-2023	8.1	Remote Procedure Call Runtime Remote Code Execution Vulnerability **CVE ID : CVE-2023-24908**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908	O-MIC-WIND-290323/3453
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability **CVE ID : CVE-2023-23401**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23401	O-MIC-WIND-290323/3454
N/A	14-Mar-2023	7.8	Windows Media Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23402	O-MIC-WIND-290323/3455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23402		
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23422**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23422	O-MIC-WIND-290323/3456
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23421**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23421	O-MIC-WIND-290323/3457
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23420**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23420	O-MIC-WIND-290323/3458
N/A	14-Mar-2023	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23417**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23417	O-MIC-WIND-290323/3459
N/A	14-Mar-2023	7.8	Windows Cryptographic Services Remote Code Execution Vulnerability **CVE ID : CVE-2023-23416**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23416	O-MIC-WIND-290323/3460
N/A	14-Mar-2023	7.8	Windows Accounts Picture Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23412**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23412	O-MIC-WIND-290323/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23423**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23423	O-MIC-WIND-290323/3462
N/A	14-Mar-2023	7.8	Windows HTTP.sys Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23410**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23410	O-MIC-WIND-290323/3463
N/A	14-Mar-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24910**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24910	O-MIC-WIND-290323/3464
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24857**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24857	O-MIC-WIND-290323/3465
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24858**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24858	O-MIC-WIND-290323/3466
N/A	14-Mar-2023	7.5	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability **CVE ID : CVE-2023-24859**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24859	O-MIC-WIND-290323/3467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	14-Mar-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24856**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24856	O-MIC-WIND-290323/3468
N/A	14-Mar-2023	7.2	Windows DNS Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-23400**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400	O-MIC-WIND-290323/3469
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23407**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23407	O-MIC-WIND-290323/3470
N/A	14-Mar-2023	7.1	Windows Point-to-Point Protocol over Ethernet (PPPoE) Remote Code Execution Vulnerability **CVE ID : CVE-2023-23414**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23414	O-MIC-WIND-290323/3471
N/A	14-Mar-2023	7	Windows Point-to-Point Protocol over Ethernet (PPPoE) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23385**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23385	O-MIC-WIND-290323/3472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows BrokerInfrastructure Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-23393**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23393	O-MIC-WIND-290323/3473
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	14-Mar-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24861**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24861	O-MIC-WIND-290323/3474
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24863**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24863	O-MIC-WIND-290323/3475
N/A	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24865**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24865	O-MIC-WIND-290323/3476
Exposure of Resource	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-290323/3477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			Disclosure Vulnerability **CVE ID : CVE-2023-24866**	ability/CVE-2023-24866	
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24870**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24870	O-MIC-WIND-290323/3478
Uncontrolled Resource Consumption	14-Mar-2023	6.5	Windows Hyper-V Denial of Service Vulnerability **CVE ID : CVE-2023-23411**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23411	O-MIC-WIND-290323/3479
Exposure of Resource to Wrong Sphere	14-Mar-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24906**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24906	O-MIC-WIND-290323/3480
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23394**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23394	O-MIC-WIND-290323/3481
Exposure of Resource to Wrong Sphere	14-Mar-2023	5.5	Client Server Run-Time Subsystem (CSRSS) Information Disclosure Vulnerability **CVE ID : CVE-2023-23409**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23409	O-MIC-WIND-290323/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	14-Mar-2023	5.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24862**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24862	O-MIC-WIND-290323/3483
N/A	14-Mar-2023	5.3	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24911**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24911	O-MIC-WIND-290323/3484
Incorrect Authorization	14-Mar-2023	4.4	Windows SmartScreen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24880**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880	O-MIC-WIND-290323/3485
Vendor: Mitsubishielectric					
Product: fx5-enet\/ip_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5--290323/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5-enet_firmware					
Affected Version(s): -					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5--290323/3487
Product: fx5s-30mr\/es_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5S-290323/3488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-30mt\/ess_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-30mt\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3490
Product: fx5s-40mr\/es_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5S-290323/3491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-40mt\/ess_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-40mt\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3493
Product: fx5s-60mr\/es_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5S-290323/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-60mt\/ess_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-60mt\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3496
Product: fx5s-80mr\/es_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5S-290323/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5s-80mt\/ess_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5s-80mt\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5S-290323/3499
Product: fx5uc-32mr\/ds-ts_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uc-32mt\/ds-ts_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uc-32mt\/dss-ts_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3502
Product: fx5uc-32mt\/dss_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uc-32mt\/d_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uc-64mt\/dss_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3505
Product: fx5uc-64mt\/d_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uc-96mt\/dss_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uc-96mt\/d_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3508
Product: fx5uj-24mr\/es-a_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-24mr\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-24mt\/es-a_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3511
Product: fx5uj-24mt\/ess_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-24mt\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-40mr\/es-a_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3514
Product: fx5uj-40mr\/es_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-40mt\/es-a_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-40mt\/ess_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3517
Product: fx5uj-40mt\/es_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-60mr\/es-a_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-60mr\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3520
Product: fx5uj-60mt\/es-a_firmware					
Affected Version(s): *					
Insufficiently	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in	https://www.mitsubishielectric.com/	O-MIT-FX5U-290323/3521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	en/psirt/vulnerability/pdf/2022-023_en.pdf	
Product: fx5uj-60mt\/ess_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**		
Product: fx5uj-60mt\/es_firmware					
Affected Version(s): *					
Insufficiently Protected Credentials	03-Mar-2023	7.5	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U(C) CPU modules all models all versions, FX5UJ CPU modules all models all versions, FX5S CPU modules all models all versions, FX5-ENET all versions and FX5-ENET/IP all versions allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server. **CVE ID : CVE-2023-0457**	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-023_en.pdf	O-MIT-FX5U-290323/3523
Vendor: Moxa					
Product: uc-2101-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	O-MOX-UC-2-290323/3524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2102-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-2-290323/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-2102-t-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-2-290323/3526
Product: uc-2104-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	O-MOX-UC-2-290323/3527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2111-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-2-290323/3528
Product: uc-2112-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	O-MOX-UC-2-290323/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2114-t-lx_firmware					
Affected Version(s): -					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-2-290323/3530
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be	N/A	O-MOX-UC-2-290323/3531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-2116-t-lx_firmware					
Affected Version(s): From (including) 1.3 Up to (including) 1.5					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-2-290323/3532
Product: uc-3101-t-ap-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can	N/A	O-MOX-UC-3-290323/3533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3101-t-eu-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3534
Product: uc-3101-t-us-lx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3535
Product: uc-3111-t-ap-lx-nw_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	O-MOX-UC-3-290323/3536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3111-t-ap-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3537
Product: uc-3111-t-eu-lx-nw_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	O-MOX-UC-3-290323/3538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3111-t-eu-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3539
Product: uc-3111-t-us-lx-nw_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	O-MOX-UC-3-290323/3540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3111-t-us-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3541
Product: uc-3121-t-ap-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	O-MOX-UC-3-290323/3542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-3121-t-eu-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-3121-t-us-lx_firmware					
Affected Version(s): From (including) 1.2 Up to (including) 2.0					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-3-290323/3544
Product: uc-5101-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	O-MOX-UC-5-290323/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5101-t-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-5-290323/3546
Product: uc-5102-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	O-MOX-UC-5-290323/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5102-t-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-5-290323/3548
Product: uc-5111-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	O-MOX-UC-5-290323/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5111-t-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-5-290323/3550
Product: uc-5112-lx_firmware					
Affected Version(s): 1.2					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	O-MOX-UC-5-290323/3551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-5112-t-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-5-290323/3552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-8112-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3553
Product: uc-8112-me-t-lx1_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	O-MOX-UC-8-290323/3554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8112-me-t-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3555
Product: uc-8112a-me-t-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	O-MOX-UC-8-290323/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8131-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3557
Product: uc-8132-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	O-MOX-UC-8-290323/3558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8162-lx_firmware					
Affected Version(s): 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3559
Product: uc-8210-t-lx-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	O-MOX-UC-8-290323/3560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8220-t-lx-ap-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-8220-t-lx-eu-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3562
Product: uc-8220-t-lx-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	O-MOX-UC-8-290323/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8220-t-lx-us-s_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3564
Product: uc-8220-t-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 2.4					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	O-MOX-UC-8-290323/3565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8410a-lx_firmware					
Affected Version(s): 2.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3566
Product: uc-8410a-nw-lx_firmware					
Affected Version(s): 2.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	O-MOX-UC-8-290323/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8410a-nw-t-lx_firmware					
Affected Version(s): 2.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3568
Product: uc-8410a-t-lx_firmware					
Affected Version(s): 2.2					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	O-MOX-UC-8-290323/3569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8540-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uc-8540-t-ct-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3571
Product: uc-8540-t-lx_firmware					
Affected Version(s): From (including) 1.0 Up to (including) 1.2					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user	N/A	O-MOX-UC-8-290323/3572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8580-lx_firmware					
Affected Version(s): 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3573
Product: uc-8580-q-lx_firmware					
Affected Version(s): 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From	N/A	O-MOX-UC-8-290323/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8580-t-ct-lx_firmware					
Affected Version(s): 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3575
Product: uc-8580-t-ct-q-lx_firmware					
Affected Version(s): 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS.	N/A	O-MOX-UC-8-290323/3576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Product: uc-8580-t-lx_firmware					
Affected Version(s): 1.1					
Improper Physical Access Control	07-Mar-2023	6.8	An attacker with physical access to the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**	N/A	O-MOX-UC-8-290323/3577
Product: uc-8580-t-q-lx_firmware					
Affected Version(s): 1.1					
Improper Physical	07-Mar-2023	6.8	An attacker with physical access to	N/A	O-MOX-UC-8-290323/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			the affected Moxa UC Series devices can initiate a restart of the device and gain access to its BIOS. Command line options can then be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device's authentication files to create a new user and gain full access to the system. **CVE ID : CVE-2023-1257**		
Vendor: Netgear					
Product: rax30_firmware					
Affected Version(s): *					
Unrestricted Upload of File with Dangerous Type	15-Mar-2023	8.8	When uploading a firmware image to a Netgear Nighthawk Wifi6 Router (RAX30), a hidden "forceFWUpdate" parameter may be provided to force the upgrade to complete and bypass certain validation checks. End users can use this to upload modified, unofficial, and potentially malicious firmware to the device. **CVE ID : CVE-2023-28337**	N/A	O-NET-RAX3-290323/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	15-Mar-2023	7.5	Any request send to a Netgear Nighthawk Wifi6 Router (RAX30)'s web service containing a “Content-Type” of “multipartboundary =” will result in the request body being written to “/tmp/mulipartFile” on the device itself. A sufficiently large file will cause device resources to be exhausted, resulting in the device becoming unusable until it is rebooted. **CVE ID : CVE-2023-28338**	N/A	O-NET-RAX3-290323/3580
Affected Version(s): * Up to (excluding) 1.0.10.94					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a buffer overflow vulnerability in various CGI mechanisms that could allow an attacker to execute arbitrary code on the device. **CVE ID : CVE-2023-27852**	N/A	O-NET-RAX3-290323/3581
Buffer Copy without Checking Size of Input	10-Mar-2023	9.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a format string vulnerability in a	N/A	O-NET-RAX3-290323/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			SOAP service that could allow an attacker to execute arbitrary code on the device. **CVE ID : CVE-2023-27853**		
Cross-Site Request Forgery (CSRF)	10-Mar-2023	8.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 is vulnerable to cross-site request forgery attacks on all endpoints due to improperly implemented CSRF protections. **CVE ID : CVE-2023-1205**	N/A	O-NET-RAX3-290323/3583
N/A	10-Mar-2023	8.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a file sharing mechanism that unintentionally allows users with upload permissions to execute arbitrary code on the device. **CVE ID : CVE-2023-27851**	N/A	O-NET-RAX3-290323/3584
N/A	10-Mar-2023	6.8	NETGEAR Nighthawk WiFi6 Router prior to V1.0.10.94 contains a file sharing mechanism that allows users with access to this feature	N/A	O-NET-RAX3-290323/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access arbitrary files on the device. **CVE ID : CVE-2023-27850**		
Affected Version(s): * Up to (excluding) 1.0.6.74					
Improper Authentication	14-Mar-2023	9.8	Netgear RAX30 (AX2400), prior to version 1.0.6.74, was affected by an authentication bypass vulnerability, allowing an unauthenticated attacker to gain administrative access to the device's web management interface by resetting the admin password. **CVE ID : CVE-2023-1327**	N/A	O-NET-RAX3-290323/3586
Vendor: Openbsd					
Product: openbsd					
Affected Version(s): 7.2					
N/A	03-Mar-2023	7.5	In OpenBSD 7.2, a TCP packet with destination port 0 that matches a pf divert-to rule can crash the kernel. **CVE ID : CVE-2023-27567**	https://ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/013_tcp.patch.sig	O-OPE-OPEN-290323/3587
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Improper Input Validation	01-Mar-2023	7.5	IBM HTTP Server 8.5 used by IBM WebSphere Application Server	https://www.ibm.com/support/pages/node/695	O-ORA-SOLA-290323/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow a remote user to cause a denial of service using a specially crafted URL. IBM X-Force ID: 248296. **CVE ID : CVE-2023-26281**	8522, https://exchange.xforce.ibmcloud.com/vulnerabilities/248296	
Vendor: poly					
Product: trio_8800_firmware					
Affected Version(s): 7.2.2.1094					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2023	5.4	An arbitrary file upload vulnerability in Poly Trio 8800 7.2.2.1094 allows attackers to execute arbitrary code via a crafted ringtone file. **CVE ID : CVE-2023-24282**	N/A	O-POL-TRIO-290323/3589
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Use of Incorrectly-Resolved Name or Reference	03-Mar-2023	7	runc through 1.1.4 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. NOTE: this issue exists because of a	N/A	O-RED-ENTE-290323/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-19921 regression. **CVE ID : CVE-2023-27561**		
Affected Version(s): 9.0					
Use of Incorrectly -Resolved Name or Reference	03-Mar-2023	7	runc through 1.1.4 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. NOTE: this issue exists because of a CVE-2019-19921 regression. **CVE ID : CVE-2023-27561**	N/A	O-RED-ENTE-290323/3591
Vendor: Samsung					
Product: exynos_1080_firmware					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3593
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3595
Buffer Copy without Checking Size of Input	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos	https://semiconductor.samsung.com/support/quality-support/pro	O-SAM-EXYN-290323/3596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	duct-security-updates/	
Product: exynos_1280_firmware					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26072		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3598
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**		
Product: exynos_2200_firmware					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3602
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980,	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-290323/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	security-updates/	
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3605
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26076		
Product: exynos_850_firmware					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3607
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3609
Buffer Copy without Checking Size of Input ('Classic	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-290323/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	security-updates/	
Product: exynos_980_firmware					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3611
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980,	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-290323/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	security-updates/	
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**		
Product: exynos_auto_t5123_firmware					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3616
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3618
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3620
Buffer Copy without Checking Size of Input ('Classic	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200,	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-290323/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**	security-updates/	
Product: exynos_modem_5123_firmware					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can lead to a denial of service. **CVE ID : CVE-2023-24033**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3622
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-290323/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	security-updates/	
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3625
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3627
Product: exynos_modem_5300_firmware					
Affected Version(s): -					
N/A	13-Mar-2023	9.8	The Samsung Exynos Modem 5123, Exynos Modem 5300, Exynos 980, Exynos 1080, and Exynos Auto T512 baseband modem chipsets do not properly check format types specified by the Session Description Protocol (SDP) module, which can	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to a denial of service. **CVE ID : CVE-2023-24033**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3629
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**		
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3631
Buffer Copy without Checking Size of Input ('Classic	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200,	https://semiconductor.samsung.com/support/quality-support/product-	O-SAM-EXYN-290323/3632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**	security-updates/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G SM message codec can occur due to insufficient parameter validation when decoding reserved options. **CVE ID : CVE-2023-26076**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3633
Product: exynos_w920_firmware					
Affected Version(s): -					
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem	https://semiconductor.samsung.com/support/quality-	O-SAM-EXYN-290323/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the Emergency number list. **CVE ID : CVE-2023-26072**	support/product-security-updates/	
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding the extended emergency number list. **CVE ID : CVE-2023-26073**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123.. A heap-based buffer overflow in the 5G MM message codec can occur due to insufficient parameter validation when decoding operator-defined access category definitions. **CVE ID : CVE-2023-26074**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3636
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Mar-2023	9.8	An issue was discovered in Samsung Mobile Chipset and Baseband Modem Chipset for Exynos 850, Exynos 980, Exynos 1080, Exynos 1280, Exynos 2200, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. An intra-object overflow in the 5G MM message codec can occur due to insufficient	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-290323/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter validation when decoding the Service Area List. **CVE ID : CVE-2023-26075**		
Vendor: sauter-controls					
Product: modunet300_ey-am300f001_firmware					
Affected Version(s): * Up to (including) 3.3-006					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	O-SAU-MODU-290323/3638
Product: modunet300_ey-am300f002_firmware					
Affected Version(s): * Up to (including) 3.3-006					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available	N/A	O-SAU-MODU-290323/3639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**		
Product: nova_106_eyk300f001_firmware					
Affected Version(s): * Up to (including) 3.3-006					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	O-SAU-NOVA-290323/3640
Product: nova_220_eyk220f001_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 3.3-006					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**	N/A	O-SAU-NOVA-290323/3641
Product: nova_230_eyk230f001_firmware					
Affected Version(s): * Up to (including) 3.3-006					
Cleartext Transmission of Sensitive Information	02-Mar-2023	7.5	SAUTER Controls Nova 200–220 Series with firmware version 3.3-006 and prior and BACnetstac version 4.2.1 and prior have only FTP and Telnet available for device management. Any sensitive information communicated through these protocols, such as credentials, is sent in cleartext. An attacker	N/A	O-SAU-NOVA-290323/3642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could obtain sensitive information such as user credentials to gain access to the system. **CVE ID : CVE-2023-0053**		
Vendor: Sonicwall					
Product: sonicos					
Affected Version(s): * Up to (excluding) 7.0.1-5111					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	O-SON-SONI-290323/3643
Affected Version(s): * Up to (including) 6.5.4.11-97n					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	O-SON-SONI-290323/3644
Affected Version(s): * Up to (including) 6.5.4.4-44v-21-1551					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes.	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	O-SON-SONI-290323/3645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1101		
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	O-SON-SONI-290323/3646
Affected Version(s): * Up to (including) 7.0.1-5083					
Improper Restriction of Excessive Authentication Attempts	02-Mar-2023	8.8	SonicOS SSLVPN improper restriction of excessive MFA attempts vulnerability allows an authenticated attacker to use excessive MFA codes. **CVE ID : CVE-2023-1101**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005	O-SON-SONI-290323/3647
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	O-SON-SONI-290323/3648
Affected Version(s): * Up to (including) 7.0.1-5111					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	02-Mar-2023	7.5	A Stack-based buffer overflow vulnerability in the SonicOS allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash. **CVE ID : CVE-2023-0656**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004	O-SON-SONI-290323/3649
Vendor: Suse					
Product: linux_enterprise_server					
Affected Version(s): 15					
NULL Pointer Dereference	01-Mar-2023	5.5	** DISPUTED ** In the Linux kernel before 6.2, mm/memory-tiers.c misinterprets the alloc_memory_type return value (expects it to be NULL in the error case, whereas it is actually an error pointer). NOTE: this is disputed by third parties because there are no realistic cases in which a user can cause the alloc_memory_type error case to be reached. **CVE ID : CVE-2023-23005**	https://github.com/torvalds/linux/commit/4a625ceee8a0ab0273534cb6b432ce6b331db5ee, https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.2, https://bugzilla.suse.com/show_bug.cgi?id=1208844#c2	O-SUS-LINU-290323/3650
Vendor: Tenda					
Product: ax3_firmware					
Affected Version(s): 16.03.12.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	15-Mar-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a stack overflow via the shareSpeed parameter at /goform/WifiGuestSet. **CVE ID : CVE-2023-27239**	N/A	O-TEN-AX3_-290323/3651
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Mar-2023	9.8	Tenda AX3 V16.03.12.11 was discovered to contain a command injection vulnerability via the lanip parameter at /goform/AdvSetLanip. **CVE ID : CVE-2023-27240**	N/A	O-TEN-AX3_-290323/3652
Product: w15e_firmware					
Affected Version(s): 15.11.0.14					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the wifiFilterListRemark parameter in the modifyWifiFilterRules function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request.	N/A	O-TEN-W15E-290323/3653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27061		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	9.8	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the DNSDomainName parameter in the formModifyDnsForward function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27063**	N/A	O-TEN-W15E-290323/3654
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	7.5	Tenda V15V1.0 was discovered to contain a buffer overflow vulnerability via the gotoUrl parameter in the formPortalAuth function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27062**	N/A	O-TEN-W15E-290323/3655
Buffer Copy without Checking Size of Input ('Classic	13-Mar-2023	7.5	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the	N/A	O-TEN-W15E-290323/3656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			index parameter in the formDelDnsForward function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27064**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Mar-2023	7.5	Tenda V15V1.0 V15.11.0.14(1521_3190_1058) was discovered to contain a buffer overflow vulnerability via the picName parameter in the formDelWewifiPi function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted request. **CVE ID : CVE-2023-27065**	N/A	O-TEN-W15E-290323/3657
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in an OS Command ('OS	08-Mar-2023	9.8	TOTOlink A7100RU V7.4cu.2313_B20191024 router has a command injection vulnerability. **CVE ID : CVE-2023-25395**	N/A	O-TOT-A710-290323/3658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Vendor: Tp-link					
Product: archer_ax21_firmware					
Affected Version(s): * Up to (excluding) 1.1.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-Mar-2023	8.8	TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 contained a command injection vulnerability in the country form of the /cgi-bin/luci;stok=/locale endpoint on the web management interface. Specifically, the country parameter of the write operation was not sanitized before being used in a call to popen(), allowing an unauthenticated attacker to inject commands, which would be run as root, with a simple POST request. **CVE ID : CVE-2023-1389**	N/A	O-TP--ARCH-290323/3659
Vendor: yoctoproject					
Product: yocto					
Affected Version(s): 3.1					
Time-of-check Time-of-use (TOCTOU)	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to	https://corp.mediatek.com/product-security-	O-YOC-YOCT-290323/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	bulletin/March-2023	
Affected Version(s): 3.3					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**	https://corp.mediatek.com/product-security-bulletin/March-2023	O-YOC-YOCT-290323/3661
Affected Version(s): 4.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	07-Mar-2023	6.4	In ion, there is a possible escalation of privilege due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/March-2023	O-YOC-YOCT-290323/3662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07559778; Issue ID: ALPS07559778. **CVE ID : CVE-2023-20623**		