National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 – 15 May 2023 Vol. 10 No. 09

Table of Content

Vendor	Product	Page Number
Qualcomm	snapdragon_wear_2500_platform	593
	snapdragon_wear_3100_platform	593
	snapdragon_wear_4100\+_platform	593
	snapdragon_x12_lte_modem	594
	snapdragon_x20_lte_modem	594
	snapdragon_x24_lte_modem	594
	snapdragon_x50_5g_modem-rf_system	595
	snapdragon_x55_5g_modem-rf_system	595
	snapdragon_x5_lte_modem	596
	snapdragon_x65_5g_modem-rf_system	596
	snapdragon_xr1_platform	596
	snapdragon_xr2\+_gen_1_platform	597
	snapdragon_xr2_5g_platform	597
	ssm7250-aa	598
	sw5100	598
	sw5100p	598
	sxr1120	598
	sxr2130	599
	wcd9326	599
	wcd9330	600
	wcd9335	600
	wcd9340	601
	wcd9341	601
	wcd9370	601
	wcd9371	602
	wcd9375	602
	wcd9380	603
	wcd9385	603
	wcn3610	604
	wcn3615	604
	wcn3620	605
	wcn3660	605

Vendor	Product	Page Number
Lenovo	thinkagile_vx3330_firmware	876
	thinkagile_vx3331_firmware	877
	thinkagile_vx3520-g_firmware	877
	thinkagile_vx3530-g_firmware	878
	thinkagile_vx3720_firmware	878
	thinkagile_vx5520_firmware	879
	thinkagile_vx5530_firmware	880
	thinkagile_vx7320_n_firmware	880
	thinkagile_vx7330_firmware	881
	thinkagile_vx7520_firmware	882
	thinkagile_vx7520_n_firmware	882
	thinkagile_vx7530_firmware	883
	thinkagile_vx7531_firmware	883
	thinkagile_vx7820_firmware	884
	thinkagile_vx_1se_firmware	885
	thinkagile_vx_2u4n_firmware	885
	thinkagile_vx_4u_firmware	886
	thinkedge_se450__firmware	887
	thinkstation_p920_firmware	887
	thinksystem_sd530_firmware	888
	thinksystem_sd630_v2_firmware	888
	thinksystem_sd650-n_v2_firmware	889
	thinksystem_sd650_firmware	890
	thinksystem_sd650_v2_firmware	890
	thinksystem_se350_firmware	891
	thinksystem_sn550_firmware	892
	thinksystem_sn550_v2_firmware	892
	thinksystem_sn850_firmware	893
	thinksystem_sr150_firmware	893
	thinksystem_sr158_firmware	894
	thinksystem_sr250_firmware	895
	thinksystem_sr250_v2_firmware	895

Vendor	Product	Page Number
Qualcomm	qca6420_firmware	984
	qca6421_firmware	984
	qca6426_firmware	985
	qca6430_firmware	985
	qca6431_firmware	986
	qca6436_firmware	986
	qca6564au_firmware	986
	qca6564a_firmware	987
	qca6564_firmware	987
	qca6574au_firmware	988
	qca6574a_firmware	988
	qca6574_firmware	989
	qca6584au_firmware	989
	qca6595au_firmware	990
	qca6595_firmware	990
	qca6696_firmware	990
	qca6698aq_firmware	991
	qca8081_firmware	991
	qca8337_firmware	992
	qca9367_firmware	992
	qca9377_firmware	993
	qca9379_firmware	993
	qcm2290_firmware	993
	qcm4290_firmware	994
	qcm6125_firmware	994
	qcm6490_firmware	995
	qcn6024_firmware	995
	qcn9011_firmware	995
	qcn9012_firmware	996
	qcn9024_firmware	996
	qcn9074_firmware	996
	qcs2290_firmware	997

Vendor	Product	Page Number
Qualcomm	qcs400_firmware	997
	qcs410_firmware	998
	qcs4290_firmware	998
	qcs605_firmware	998
	qcs610_firmware	999
	qcs6125_firmware	999
	qcs6490_firmware	1000
	qcs8155_firmware	1000
	qcs8250_firmware	1001
	qm215_firmware	1001
	qrb5165m_firmware	1001
	qrb5165n_firmware	1002
	qrb5165_firmware	1002
	qsm8250_firmware	1003
	sa4150p_firmware	1003
	sa4155p_firmware	1003
	sa6145p_firmware	1004
	sa6150p_firmware	1004
	sa6155p_firmware	1005
	sa6155_firmware	1005
	sa8145p_firmware	1006
	sa8150p_firmware	1007
	sa8155p_firmware	1007
	sa8155_firmware	1008
	sa8195p_firmware	1008
	sa8295p_firmware	1009
	sa8540p_firmware	1009
	sa9000p_firmware	1010
	sd626_firmware	1010
	sd660_firmware	1010
	sd670_firmware	1011
	sd675_firmware	1011

Vendor	Product	Page Number
Qualcomm	sd730_firmware	1012
	sd835_firmware	1012
	sd855_firmware	1013
	sd865_5g_firmware	1013
	sd888_firmware	1014
	sda\/sdm845_firmware	1014
	sdm429w_firmware	1014
	sdm429_firmware	1015
	sdm439_firmware	1015
	sdm450_firmware	1016
	sdm660_firmware	1016
	sdm670_firmware	1017
	sdm710_firmware	1017
	sdm845_firmware	1017
	sdx20m_firmware	1018
	sdx55_firmware	1018
	sd_675_firmware	1019
	sm4125_firmware	1019
	sm4250-aa_firmware	1020
	sm4350-ac_firmware	1020
	sm4350_firmware	1020
	sm4375_firmware	1021
	sm6115_firmware	1021
	sm6125_firmware	1021
	sm6150-ac_firmware	1022
	sm6150_firmware	1022
	sm6225-ad_firmware	1023
	sm6225_firmware	1023
	sm6250p_firmware	1024
	sm6250_firmware	1024
	sm6350_firmware	1025
	sm6375_firmware	1025

Vendor	Product	Page Number
Qualcomm	sm7125_firmware	1025
	sm7150-aa_firmware	1026
	sm7150-ab_firmware	1026
	sm7150-ac_firmware	1027
	sm7225_firmware	1027
	sm7250-aa_firmware	1028
	sm7250-ab_firmware	1028
	sm7250-ac_firmware	1028
	sm7250p_firmware	1029
	sm7315_firmware	1029
	sm7325-ae_firmware	1029
	sm7325-af_firmware	1030
	sm7325p_firmware	1030
	sm7325_firmware	1030
	sm7350-ab_firmware	1030
	sm8150-ac_firmware	1031
	sm8150_firmware	1031
	sm8250-ab_firmware	1031
	sm8250-ac_firmware	1032
	sm8250_firmware	1032
	sm8350-ac_firmware	1032
	sm8350_firmware	1033
	snapdragon_1200_wearable_platform_firmware	1033
	snapdragon_208_processor_firmware	1033
	snapdragon_630_mobile_platform_firmware	1034
	snapdragon_632_mobile_platform_firmware	1034
	snapdragon_636_mobile_platform_firmware	1034
	snapdragon_7c\+_gen_3_compute_firmware	1035
	snapdragon_820_automotive_platform_firmware	1035
	snapdragon_auto_4g_modem_firmware	1035
	snapdragon_auto_5g_modem-rf_firmware	1036

Vendor	Product	Page Number
Qualcomm	snapdragon_w5\+_gen_1_wearable_platform_firmware	1036
	snapdragon_wear_2100_platform_firmware	1036
	snapdragon_wear_2500_platform_firmware	1037
	snapdragon_wear_3100_platform_firmware	1037
	snapdragon_wear_4100\+_platform_firmware	1037
	snapdragon_x12_lte_modem_firmware	1038
	snapdragon_x20_lte_modem_firmware	1038
	snapdragon_x24_lte_modem_firmware	1038
	snapdragon_x50_5g_modem-rf_system_firmware	1039
	snapdragon_x55_5g_modem-rf_system_firmware	1039
	snapdragon_x5_lte_modem_firmware	1040
	snapdragon_x65_5g_modem-rf_system_firmware	1040
	snapdragon_xr1_platform_firmware	1040
	snapdragon_xr2\+_gen_1_platform_firmware	1041
	snapdragon_xr2_5g_platform_firmware	1041
	ssm7250-aa_firmware	1042
	sw5100p_firmware	1042
	sw5100_firmware	1042
	sxr1120_firmware	1043
	sxr2130_firmware	1043
	wcd9326_firmware	1043
	wcd9330_firmware	1044
	wcd9335_firmware	1044
	wcd9340_firmware	1045
	wcd9341_firmware	1045
	wcd9370_firmware	1046
	wcd9371_firmware	1046
	wcd9375_firmware	1047
	wcd9380_firmware	1047

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 8web					
Product: read_more_without_refresh					
Affected Version(s): * Up to (excluding) 3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eightweb Interactive Read More Without Refresh plugin <= 3.1 versions. **CVE ID : CVE-2023-23793**	N/A	A-8WE-READ-170523/1
Vendor: 9seeds					
Product: cpt_-_speakers					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in 9seeds.Com CPT – Speakers plugin <= 1.1 versions. **CVE ID : CVE-2023-25977**	N/A	A-9SE-CPT_-170523/2
Vendor: advancedcustomfields					
Product: advanced_custom_fields					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.12.5					
Deserialization of Untrusted Data	02-May-2023	8.8	The Advanced Custom Fields (ACF) Free and Pro WordPress plugins 6.x before 6.1.0 and 5.x before 5.12.5 unserialize user controllable data,	N/A	A-ADV-ADVA-170523/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could allow users with a role of Contributor and above to perform PHP Object Injection when a suitable gadget is present. **CVE ID : CVE-2023-1196**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.1.0					
Deserialization of Untrusted Data	02-May-2023	8.8	The Advanced Custom Fields (ACF) Free and Pro WordPress plugins 6.x before 6.1.0 and 5.x before 5.12.5 unserialize user controllable data, which could allow users with a role of Contributor and above to perform PHP Object Injection when a suitable gadget is present. **CVE ID : CVE-2023-1196**	N/A	A-ADV-ADVA-170523/4
Vendor: agentevolution					
Product: impress_listings					
Affected Version(s): * Up to (including) 2.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Agent Evolution IMPress Listings plugin <= 2.6.2 versions. **CVE ID : CVE-2023-22711**	N/A	A-AGE-IMPR-170523/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: agilepoint					
Product: agilepoint_nx					
Affected Version(s): 8.0					
Unrestricted Upload of File with Dangerous Type	08-May-2023	9.8	AgilePoint NX v8.0 SU2.2 & SU2.3 – Insecure File Upload - Vulnerability allows insecure file upload, by an unspecified request. **CVE ID : CVE-2023-24507**	N/A	A-AGI-AGIL-170523/6
N/A	08-May-2023	9.1	AgilePoint NX v8.0 SU2.2 & SU2.3 – Arbitrary File Delete Vulnerability allows arbitrary file deletion, by an unspecified request. **CVE ID : CVE-2023-31178**	N/A	A-AGI-AGIL-170523/7
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-May-2023	7.5	AgilePoint NX v8.0 SU2.2 & SU2.3 - Path traversal - Vulnerability allows path traversal and downloading files from the server, by an unspecified request.	N/A	A-AGI-AGIL-170523/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31179		
Vendor: Amazon					
Product: opensearch					
Affected Version(s): * Up to (excluding) 1.3.10					
Incorrect Authorization	08-May-2023	5.9	OpenSearch is open-source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue.	https://github.com/opensearch-project/security/security/advisories/GHSA-g8xc-6mf7-h28h	A-AMA-OPEN-170523/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31141		
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.7.0					
Incorrect Authorization	08-May-2023	5.9	OpenSearch is open-source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue. **CVE ID : CVE-2023-31141**	https://github.com/opensearch-project/security/security/advisories/GHSA-g8xc-6mf7-h28h	A-AMA-OPEN-170523/10
Product: opensearch_security					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.3.10					
Incorrect Authorization	08-May-2023	5.9	OpenSearch is open-source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue. **CVE ID : CVE-2023-31141**	https://github.com/opensearch-project/security/security/advisories/GHSA-g8xc-6mf7-h28h	A-AMA-OPEN-170523/11
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	08-May-2023	5.9	OpenSearch is open-source software suite for search, analytics, and observability applications. Prior to versions 1.3.10 and 2.7.0, there is an issue with the implementation of fine-grained access control rules (document-level security, field-level security and field masking) where they are not correctly applied to the queries during extremely rare race conditions potentially leading to incorrect access authorization. For this issue to be triggered, two concurrent requests need to land on the same instance exactly when query cache eviction happens, once every four hours. OpenSearch 1.3.10 and 2.7.0 contain a fix for this issue. **CVE ID : CVE-2023-31141**	https://github.com/opensearch-project/security/security/advisories/GHSA-g8xc-6mf7-h28h	A-AMA-OPEN-170523/12
Vendor: amr-ical-events-list_project					
Product: amr-ical-events-list					
Affected Version(s): * Up to (including) 6.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	The amr ical events lists WordPress plugin through 6.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-1021**	N/A	A-AMR-AMR--170523/13
Vendor: answer					
Product: answer					
Affected Version(s): * Up to (excluding) 1.0.9					
Missing Authorization	09-May-2023	3.5	Missing Authorization in GitHub repository answerdev/answer prior to 1.0.9. **CVE ID : CVE-2023-2590**	https://hunter.dev/bounties/a4238a30-3ddb-4415-9055-e179c3d4dea7, https://github.com/answerdev/answer/commit/51ac1e6b76ae9ab3ca2008ca4819c0cc3bd2fcd3	A-ANS-ANSW-170523/14
Vendor: antabot_white-jotter_project					
Product: antabot_white-jotter					
Affected Version(s): 0.2.2					
Unrestricted Upload of	01-May-2023	9.8	File upload vulnerability in	https://github.com/Antab	A-ANT-ANTA-170523/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			Antabot White-Jotter v0.2.2, allows remote attackers to execute malicious code via the file parameter to function coversUpload. **CVE ID : CVE-2023-29635**	ot/White-Jotter/issues/157, https://github.com/Antabot/White-Jotter/blob/c1c5d66fda090b986b8f46a7132d403e3b038c5d/wj/src/main/java/com/gm/wj/controller/LibraryController.java#L63	
Vendor: Apache					
Product: airflow					
Affected Version(s): * Up to (excluding) 2.6.0					
N/A	08-May-2023	9.8	Privilege Context Switching Error vulnerability in Apache Software Foundation Apache Airflow.This issue affects Apache Airflow: before 2.6.0. **CVE ID : CVE-2023-25754**	https://github.com/apache/airflow/pull/29506	A-APA-AIRF-170523/16
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Task instance details page in the UI is vulnerable to a stored XSS.This issue affects Apache Airflow: before 2.6.0.	https://github.com/apache/airflow/pull/30779, https://github.com/apache/airflow/pull/30447	A-APA-AIRF-170523/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29247		
Product: brpc					
Affected Version(s): From (including) 0.9.0 Up to (excluding) 1.5.0					
Improper Input Validation	08-May-2023	9.8	Security vulnerability in Apache bRPC <1.5.0 on all platforms allows attackers to execute arbitrary code via ServerOptions::pid_file. An attacker that can influence the ServerOptions pid_file parameter with which the bRPC server is started can execute arbitrary code with the permissions of the bRPC process. Solution: 1. upgrade to bRPC >= 1.5.0, download link: https://dist.apache.org/repos/dist/release/brpc/1.5.0/ https://dist.apache.org/repos/dist/release/brpc/1.5.0/ 2. If you are using an old version of bRPC and hard to upgrade, you can apply this patch: https://github.com/apache/brpc/pull/2218	https://lists.apache.org/thread/jqpttrqbc38yhckgp67xk399hqxnz7jn, http://www.openwall.com/lists/oss-security/2023/05/08/1	A-APA-BRPC-170523/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			https://github.com/apache/brpc/pull/2218 **CVE ID : CVE-2023-31039**		
Product: couchdb					
Affected Version(s): * Up to (excluding) 3.2.3					
N/A	02-May-2023	5.3	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when using these design document functions: * validate_doc_update * list * filter * filter views (using view functions as filters) * rewrite * update This doesn't affect map/reduce or	https://docs.couchdb.org/en/stable/cve/2023-26268.html	A-APA-COUC-170523/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			search (Dreyfus) index functions. Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3). Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store data in the Javascript environment. **CVE ID : CVE-2023-26268**		
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.2					
N/A	02-May-2023	5.3	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when using these design document functions: * validate_doc_update * list	https://docs.couchdb.org/en/stable/cve/2023-26268.html	A-APA-COUC-170523/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* filter * filter views (using view functions as filters) * rewrite * update This doesn't affect map/reduce or search (Dreyfus) index functions. Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3). Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store data in the Javascript environment. **CVE ID : CVE-2023-26268**		
Product: log4cxx					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 0.9.0 Up to (excluding) 1.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-May-2023	8.8	SQL injection in Log4cxx when using the ODBC appender to send log messages to a database. No fields sent to the database were properly escaped for SQL injection. This has been the case since at least version 0.9.0(released 2003-08-06) Note that Log4cxx is a C++ framework, so only C++ applications are affected. Before version 1.1.0, the ODBC appender was automatically part of Log4cxx if the library was found when compiling the library. As of version 1.1.0, this must be both explicitly enabled in order to be compiled in.	https://lists.apache.org/thread/vgjlpdf353vv91gryspwxrzj6p0fbjd9	A-APA-LOG4-170523/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Three preconditions must be met for this vulnerability to be possible: 1. Log4cxx compiled with ODBC support(before version 1.1.0, this was auto-detected at compile time) 2. ODBCAppender enabled for logging messages to, generally done via a config file 3. User input is logged at some point. If your application does not have user input, it is unlikely to be affected. Users are recommended to upgrade to version 1.1.0 which properly binds the parameters to the SQL statement, or migrate to the new DBAppender class which supports an ODBC connection		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in addition to other databases. Note that this fix does require a configuration file update, as the old configuration files will not configure properly. An example is shown below, and more information may be found in the Log4cxx documentation on the ODBCAppender. Example of old configuration snippet: <appender name="SqlODBCAppender" class="ODBCAppender"> <param name="sql" value="INSERT INTO logs (message) VALUES ('%m')" /> ... other params here ...		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			</appender> The migrated configuration snippet with new ColumnMapping parameters: <appender name="SqlODBCAppender" class="ODBCAppender"> <param name="sql" value="INSERT INTO logs (message) VALUES (?)" /> <param name="ColumnMapping" value="message"/> ... other params here ... </appender>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31038		
Product: spark					
Affected Version(s): * Up to (including) 3.0.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-May-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will	https://spark.apache.org/security.html	A-APA-SPAR-170523/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022-33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0. **CVE ID : CVE-2023-32007**		
Affected Version(s): From (including) 3.1.1 Up to (including) 3.1.3					
Improper Neutralization of Special Elements used in a Command ('Comman	02-May-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable.	https://spark.apache.org/security.html	A-APA-SPAR-170523/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022-33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected. NOTE: This vulnerability only affects products that are no longer		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supported by the maintainer. Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0. **CVE ID : CVE-2023-32007**		
Affected Version(s): From (including) 3.2.0 Up to (including) 3.2.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	02-May-2023	8.8	** UNSUPPORTED WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission	https://spark.apache.org/security.html	A-APA-SPAR-170523/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022-33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0. **CVE ID : CVE-2023-32007**		
Vendor: appim					
Product: appium-desktop					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.22.3-4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-May-2023	9.8	OS Command Injection in GitHub repository appium/appium-desktop prior to v1.22.3-4. **CVE ID : CVE-2023-2479**	https://hunter.dev/bounties/fbdeec3c-d197-4a68-a547-7f93fb9594b4, https://github.com/appium/appium-desktop/commit/12a988aa08b9822e97056a09486c9bebb3aad8fe	A-APP-APPI-170523/25
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 16.4					
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-28201**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213676	A-APP-SAFA-170523/26
N/A	08-May-2023	6.5	The issue was addressed by	https://support.apple.co	A-APP-SAFA-170523/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	m/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
Product: xcode					
Affected Version(s): * Up to (excluding) 14.3					
N/A	08-May-2023	8.6	The issue was addressed with improved memory handling. This issue is fixed in Xcode 14.3. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges	https://support.apple.com/en-us/HT213679	A-APP-XCOD-170523/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27967		
N/A	08-May-2023	6.3	This issue was addressed with improved entitlements. This issue is fixed in Xcode 14.3. A sandboxed app may be able to collect system logs **CVE ID : CVE-2023-27945**	https://support.apple.com/en-us/HT213679	A-APP-XCOD-170523/29
Vendor: archerirm					
Product: archer					
Affected Version(s): From (including) 6.12.0.0 Up to (excluding) 6.12.0.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	5.4	Archer Platform 6.8 before 6.12 P6 HF1 (6.12.0.6.1) contains a stored XSS vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. 6.11.P4 (6.11.0.4) is also a fixed release. **CVE ID : CVE-2023-30639**	https://www.archerirm.community/t5/security-advisories/archer-update-for-stored-cross-site-scripting/ta-p/697581	A-ARC-ARCH-170523/30
Affected Version(s): From (including) 6.8.0.0 Up to (including) 6.11.0.4					
Improper Neutralization of Input	01-May-2023	5.4	Archer Platform 6.8 before 6.12 P6 HF1 (6.12.0.6.1) contains a stored XSS	https://www.archerirm.community/t5/security-	A-ARC-ARCH-170523/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability. A remote authenticated malicious Archer user could potentially exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. 6.11.P4 (6.11.0.4) is also a fixed release. **CVE ID : CVE-2023-30639**	advisories/archer-update-for-stored-cross-site-scripting/tap/697581	
Vendor: artisanworkshop					
Product: japanized_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.5.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	The Japanized For WooCommerce WordPress plugin before 2.5.8 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2023-0948**	N/A	A-ART-JAPA-170523/32
Vendor: asmbb_project					
Product: asmbb					
Affected Version(s): 2.9.1					
Improper Neutralization of Input During Web Page Generation	08-May-2023	6.1	AsmBB v2.9.1 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities via the MiniMag.asm	https://asm32.info/fossil/asmbb/info/7dfa4f56b473f76c, https://fresh.flatassemble	A-ASM-ASMB-170523/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			and bbcode.asm libraries. **CVE ID : CVE-2023-30334**	r.net/fossil/repo/fresh/info/a3caaf7ad8503348	
Vendor: Atlassian					
Product: confluence_data_center					
Affected Version(s): * Up to (excluding) 7.13.15					
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. **CVE ID : CVE-2023-22503**	https://jira.atlassian.com/browse/CONFSERVER-82403	A-ATL-CONF-170523/34
Affected Version(s): From (including) 7.14.0 Up to (excluding) 7.19.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. **CVE ID : CVE-2023-22503**	https://jira.atlassian.com/browse/CONFSERVER-82403	A-ATL-CONF-170523/35
Affected Version(s): From (including) 7.20.0 Up to (excluding) 8.2.0					
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space.	https://jira.atlassian.com/browse/CONFSERVER-82403	A-ATL-CONF-170523/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. **CVE ID : CVE-2023-22503**		
Product: confluence_server					
Affected Version(s): * Up to (excluding) 7.13.15					
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature.	https://jira.atlassian.com/browse/CONFSERVER-82403	A-ATL-CONF-170523/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. **CVE ID : CVE-2023-22503**		
Affected Version(s): From (including) 7.14.0 Up to (excluding) 7.19.7					
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version	https://jira.atlassian.com/browse/CONFSERVER-82403	A-ATL-CONF-170523/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. **CVE ID : CVE-2023-22503**		
Affected Version(s): From (including) 7.20.0 Up to (excluding) 8.2.0					
N/A	01-May-2023	5.3	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature. This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0. **CVE ID : CVE-2023-22503**	https://jira.atlassian.com/browse/CONFSERVER-82403	A-ATL-CONF-170523/39
Vendor: avirato					
Product: hotels_online_booking_engine					
Affected Version(s): * Up to (including) 5.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-May-2023	8.8	The Avirato hotels online booking engine WordPress plugin through 5.0.5 does not validate and escape some of its shortcode attributes before using them in SQL statement/s, which could allow any authenticated users, such as subscriber to perform SQL Injection attacks. **CVE ID : CVE-2023-0768**	N/A	A-AVI-HOTE-170523/40
Vendor: azuracast					
Product: azuracast					
Affected Version(s): * Up to (excluding) 0.18.3					
Improper Restriction of Excessive Authentication Attempts	05-May-2023	9.8	Improper Restriction of Excessive Authentication Attempts in GitHub repository azuracast/azuracast prior to 0.18.3. **CVE ID : CVE-2023-2531**	https://huntr.dev/bounties/20463eb2-0f9d-4ea3-a2c8-93f80e7aca02, https://github.com/azuracast/azuracast/commit/bdb23594ad3e0c47c8568ce028a7c244a406cf9d	A-AZU-AZUR-170523/41
Vendor: basixonline					
Product: nex-forms					
Affected Version(s): * Up to (excluding) 8.4					
Improper Neutralization of	08-May-2023	7.2	The NEX-Forms WordPress plugin before 8.4 does not	N/A	A-BAS-NEX--170523/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			properly escape the `table` parameter, which is populated with user input, before concatenating it to an SQL query. **CVE ID : CVE-2023-2114**		
Vendor: beetl_project					
Product: beetl					
Affected Version(s): 3.15					
N/A	04-May-2023	9.8	An issue in the render function of beetl v3.15.0 allows attackers to execute server-side template injection (SSTI) via a crafted payload. **CVE ID : CVE-2023-30331**	N/A	A-BEE-BEET-170523/43
Vendor: billing_management_system_project					
Product: billing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-May-2023	9.8	A vulnerability has been found in SourceCodester Billing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file ajax_service.php of the component POST Parameter Handler. The manipulation of the argument drop_services leads to sql injection. The	N/A	A-BIL-BILL-170523/44

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 identifier VDB-228397 was assigned to this vulnerability. **CVE ID : CVE-2023-2595**		
Vendor: bing_site_verification_plugin_using_meta_tag_project					
Product: bing_site_verification_plugin_using_meta_tag					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Himanshu Bing Site Verification plugin using Meta Tag plugin <= 1.0 versions. **CVE ID : CVE-2023-23875**	N/A	A-BIN-BING-170523/45
Vendor: blackandwhitedigital					
Product: treepress					
Affected Version(s): * Up to (excluding) 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Black and White Digital Ltd TreePress – Easy Family Trees & Ancestor Profiles plugin <= 2.0.22 versions. **CVE ID : CVE-2023-23863**	N/A	A-BLA-TREE-170523/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: blueglass					
Product: jobs_for_wordpress					
Affected Version(s): * Up to (excluding) 2.5.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BlueGlass Jobs for WordPress plugin <= 2.5.10.2 versions. **CVE ID : CVE-2023-26017**	N/A	A-BLU-JOBS-170523/47
Vendor: booqable					
Product: rental_software_booqable_rental					
Affected Version(s): * Up to (including) 2.4.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Booqable Rental Software Booqable Rental plugin <= 2.4.15 versions. **CVE ID : CVE-2023-30746**	N/A	A-BOO-RENT-170523/48
Vendor: bumsys_project					
Product: bumsys					
Affected Version(s): * Up to (excluding) 2.1.1					
Inclusion of Functionality from Untrusted Control Sphere	05-May-2023	8.8	PHP Remote File Inclusion in GitHub repository unilogies/bumsys prior to 2.1.1. **CVE ID : CVE-2023-2551**	https://github.com/unilogies/bumsys/commit/86e29dd23df348ec6075f0c0de8e06b8d9fb0a9a, https://huntr.dev/bounties/5723613	A-BUM-BUMS-170523/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				c-55c6-4f18-9ed3-61ad44f5de9c	
Cross-Site Request Forgery (CSRF)	05-May-2023	8.8	Cross-Site Request Forgery (CSRF) in GitHub repository unilogies/bumsys prior to 2.1.1. **CVE ID : CVE-2023-2552**	https://huntr.dev/bounties/ab0b4655-f57a-4113-849b-2237eeb75b32, https://github.com/unilogies/bumsys/commit/86e29dd23df348ec6075f0c0de8e06b8d9fb0a9a	A-BUM-BUMS-170523/50
Affected Version(s): * Up to (excluding) 2.2.0					
External Control of File Name or Path	05-May-2023	7.2	External Control of File Name or Path in GitHub repository unilogies/bumsys prior to 2.2.0. **CVE ID : CVE-2023-2554**	https://huntr.dev/bounties/396785a0-7bb6-4db4-b4cb-607b0fd4ab4b, https://github.com/unilogies/bumsys/commit/1b426f58a513194206d0ea8ab58baf1461e54978	A-BUM-BUMS-170523/51
Improper Neutralization of Input During Web Page Generation	05-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository unilogies/bumsys prior to 2.2.0. **CVE ID : CVE-2023-2553**	https://huntr.dev/bounties/4e1f5b56-e846-40d8-a83c-533efd56aacf, https://githu	A-BUM-BUMS-170523/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				b.com/unilogies/bumsys/commit/1b426f58a513194206d0ea8ab58baf1461e54978	
Vendor: byconsole					
Product: pickup_|_delivery_|_dine-in_date_time					
Affected Version(s): * Up to (including) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	The Pickup | Delivery | Dine-in date time WordPress plugin through 1.0.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-0894**	N/A	A-BYC-PICK-170523/53
Vendor: catchthemes					
Product: darcie					
Affected Version(s): * Up to (excluding) 1.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Catch Themes Darcie theme <= 1.1.5 versions. **CVE ID : CVE-2023-25961**	N/A	A-CAT-DARC-170523/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: catontechnology					
Product: caton_prime					
Affected Version(s): 2.1.2.51.e8d7225049\\(202303031001\\)					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-May-2023	9.8	A vulnerability was found in Caton Prime 2.1.2.51.e8d7225049 (202303031001) and classified as critical. This issue affects some unknown processing of the file cgi-bin/tools_ping.cgi?action=Command of the component Ping Handler. The manipulation of the argument Destination leads to command injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-228011. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2520**	N/A	A-CAT-CATO-170523/55
Product: ctp_relay_server					
Affected Version(s): 1.2.9					
Improper Neutralization of Special Elements used in an SQL	04-May-2023	9.8	A vulnerability has been found in Caton CTP Relay Server 1.2.9 and classified as critical. This vulnerability affects unknown code of the	N/A	A-CAT-CTP_-170523/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			file /server/api/v1/login of the component API. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. VDB-228010 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2519**		
Vendor: Cesanta					
Product: mjs					
Affected Version(s): 1.26					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-May-2023	5.5	An issue found in Cesanta MJS v.1.26 allows a local attacker to cause a denial of service via the mjs_execute function in mjs.c. **CVE ID : CVE-2023-30088**	https://github.com/cesanta/mjs/issues/243	A-CES-MJS-170523/57
Vendor: Chamilo					
Product: chamilo_lms					
Affected Version(s): 1.11.18					
Improper Neutralization of Input During Web Page	09-May-2023	6.1	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues	A-CHA-CHAM-170523/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code via the skills wheel parameter. **CVE ID : CVE-2023-31801**	#Issue-97-2023-04-11-Low-impact-High-risk-XSS-in-skills-wheel	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the forum title parameter. **CVE ID : CVE-2023-31800**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-102-2023-04-11-Low-impact-Moderate-risk-XSS-in-forum-titles	A-CHA-CHAM-170523/59
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the skype and linedin_url parameters. **CVE ID : CVE-2023-31802**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-104-2023-04-11-Moderate-impact-High-risk-XSS-in-personal-profile	A-CHA-CHAM-170523/60
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the course category parameters. **CVE ID : CVE-2023-31804**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-96-2023-04-06-Low-impact-Moderate-risk-XSS-in-	A-CHA-CHAM-170523/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				course-categories	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via a crafted payload to the My Progress function. **CVE ID : CVE-2023-31806**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-103-2023-04-11-Low-impact-Moderate-risk-XSS-in-My-progress-tab	A-CHA-CHAM-170523/62
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via a crafted payload to the personal notes function. **CVE ID : CVE-2023-31807**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-101-2023-04-11-Low-impact-Low-risk-XSS-in-personal-notes-and-teacher-notes	A-CHA-CHAM-170523/63
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the system annnouncements parameter. **CVE ID : CVE-2023-31799**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-99-2023-04-11-Low-impact-Low-risk-XSS-in-system-	A-CHA-CHAM-170523/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				announcements	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local attacker to execute arbitrary code via the resource sequencing parameters. **CVE ID : CVE-2023-31803**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-100-2023-04-11-Low-impact-Low-risk-XSS-in-resources-sequencing	A-CHA-CHAM-170523/65
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Cross Site Scripting vulnerability found in Chamilo Lms v.1.11.18 allows a local authenticated attacker to execute arbitrary code via the homepage function. **CVE ID : CVE-2023-31805**	https://support.chamilo.org/projects/chamilo-18/wiki/Security_issues#Issue-98-2023-04-11-Low-impact-Low-risk-XSS-in-homepage-edition	A-CHA-CHAM-170523/66
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): 4.5.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	9.8	ChurchCRM 4.5.4 endpoint /EditEventTypes.php is vulnerable to Blind SQL Injection (Time-based) via the EN_tyid POST parameter. **CVE ID : CVE-2023-29842**	N/A	A-CHU-CHUR-170523/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: clio					
Product: clio_grow					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themis Solutions, Inc. Clio Grow plugin <= 1.0.0 versions. **CVE ID : CVE-2023-22683**	N/A	A-CLI-CLIO-170523/68
Vendor: cloud_manager_project					
Product: cloud_manager					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	The Cloud Manager WordPress plugin through 1.0 does not sanitise and escape the query param ricerca before outputting it in an admin panel, allowing unauthenticated attackers to trick a logged in admin to trigger a XSS payload by clicking a link. **CVE ID : CVE-2023-0421**	N/A	A-CLO-CLOU-170523/69
Vendor: cltphp					
Product: cltphp					
Affected Version(s): * Up to (including) 6.0					
Unrestricted Upload of File with Dangerous Type	04-May-2023	9.8	CLTPHP <=6.0 is vulnerable to Unrestricted Upload of File with Dangerous Type via	N/A	A-CLT-CLTP-170523/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application/admin/controller/Template.php:update. **CVE ID : CVE-2023-30264**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-May-2023	9.8	CLTPHP <=6.0 is vulnerable to Improper Input Validation. **CVE ID : CVE-2023-30268**	N/A	A-CLT-CLTP-170523/71
Vendor: cms_press_project					
Product: cms_press					
Affected Version(s): * Up to (including) 0.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Michael Pretty (prettyboymp) CMS Press plugin <= 0.2.3 versions. **CVE ID : CVE-2023-25452**	N/A	A-CMS-CMS_-170523/72
Vendor: codestag					
Product: stagtools					
Affected Version(s): * Up to (excluding) 2.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The StagTools WordPress plugin before 2.3.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which	N/A	A-COD-STAG-170523/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0891**		
Vendor: controlid					
Product: rhid					
Affected Version(s): 23.3.19.0					
Direct Request ('Forced Browsing')	04-May-2023	9.8	A vulnerability classified as critical has been found in Control iD RHiD 23.3.19.0. This affects an unknown part of the file /v2/#/. The manipulation leads to direct request. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-228015. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2524**	N/A	A-CON-RHID-170523/74
Vendor: convertbox					
Product: convertbox_auto_embed					
Affected Version(s): * Up to (excluding) 1.0.20					
Improper Neutralization of Input	09-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in	N/A	A-CON-CONV-170523/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			ConvertBox ConvertBox Auto Embed WordPress plugin <= 1.0.19 versions. **CVE ID : CVE-2023-23664**		
Vendor: creativethemes					
Product: blocksy_companion					
Affected Version(s): * Up to (excluding) 1.8.82					
Authorization Bypass Through User-Controlled Key	02-May-2023	4.3	The Blocksy Companion WordPress plugin before 1.8.82 does not ensure that posts to be accessed via a shortcode are already public and can be viewed, allowing any authenticated users, such as subscriber to access draft posts for example **CVE ID : CVE-2023-1911**	N/A	A-CRE-BLOC-170523/76
Vendor: crmeb					
Product: crmeb					
Affected Version(s): From (including) 4.4.0 Up to (including) 4.6.0					
Unrestricted Upload of File with Dangerous Type	08-May-2023	9.8	CRMEB v4.4 to v4.6 was discovered to contain an arbitrary file upload vulnerability via the component \attachment\SystemAttachmentServices.php. **CVE ID : CVE-2023-30185**	N/A	A-CRM-CRME-170523/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: custom_login_page_project					
Product: custom_login_page					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Denzel Chia | Phire Design Custom Login Page plugin <= 2.0 versions. **CVE ID : CVE-2023-26012**	N/A	A-CUS-CUST-170523/78
Vendor: custom_more_link_complete_project					
Product: custom_more_link_complete					
Affected Version(s): * Up to (including) 1.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Florin Arjocu Custom More Link Complete plugin <= 1.4.1 versions. **CVE ID : CVE-2023-23788**	N/A	A-CUS-CUST-170523/79
Vendor: cybonet					
Product: pineapp_mail_secure					
Affected Version(s): * Up to (excluding) 1.0.10.1646					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	Cybonet PineApp Mail Secure A reflected cross-site scripting (XSS) vulnerability was identified in the product, using an unspecified endpoint.	N/A	A-CYB-PINE-170523/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31183		
Vendor: Dell					
Product: alienware_command_center					
Affected Version(s): * Up to (excluding) 5.5.46.0					
Improper Access Control	03-May-2023	7.8	Alienware Command Center Application, versions 5.5.43.0 and prior, contain an improper access control vulnerability. A local malicious user could potentially exploit this vulnerability during installation or update process leading to privilege escalation. **CVE ID : CVE-2023-28070**	https://www.dell.com/support/kbdoc/en-us/000212277/dsa-2023-135	A-DEL-ALIE-170523/81
Product: command_|_monitor					
Affected Version(s): * Up to (including) 10.9					
Incorrect Permission Assignment for	05-May-2023	7.8	Dell Command Monitor, versions 10.9 and prior, contains an	https://www.dell.com/support/kbdoc/en-us/0002122	A-DEL-COMM-170523/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			improper folder permission vulnerability. A local authenticated malicious user can potentially exploit this vulnerability leading to privilege escalation by writing to a protected directory when Dell Command Monitor is installed to a non-default path **CVE ID : CVE-2023-28068**	26/dsa-2023-133	
Product: elastic_cloud_storage					
Affected Version(s): * Up to (excluding) 3.8.0.2					
Improper Verification of Cryptographic Signature	04-May-2023	7.5	DELL ECS prior to 3.8.0.2 contains an improper verification of cryptographic signature vulnerability. A network attacker with an ability to intercept the request could potentially exploit this vulnerability to modify the body data of the request. **CVE ID : CVE-2023-25934**	https://www.dell.com/support/kbdoc/en-us/000212970/dsa-2023-109-dell-ecs-security-update-for-multiple-vulnerabilities	A-DEL-ELAS-170523/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2023.1.3.0					
N/A	02-May-2023	4.9	Improper access control in Subscriptions Folder path filter in Devolutions Server 2023.1.1 and earlier allows attackers with administrator privileges to retrieve usage information on folders in user vaults via a specific folder name. **CVE ID : CVE-2023-2445**	https://devolutions.net/security/advisories/DEVO-2023-0013/	A-DEV-DEVO-170523/84
Vendor: digitaldruid					
Product: hotel_druid					
Affected Version(s): 3.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A Stored Cross Site Scripting (XSS) vulnerability exists in multiple pages of Hotel Druid version 3.0.4, which allows arbitrary execution of commands. The vulnerable fields are Surname, Name, and Nickname in the Document function. **CVE ID : CVE-2023-29839**	N/A	A-DIG-HOTE-170523/85
Vendor: disqus_conditional_load_project					
Product: disqus_conditional_load					
Affected Version(s): * Up to (including) 11.0.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joel James Disqus Conditional Load plugin <= 11.0.6 versions. **CVE ID : CVE-2023-23732**	N/A	A-DIS-DISQ-170523/86
Vendor: Djangoproject					
Product: django					
Affected Version(s): 4.2					
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. **CVE ID : CVE-2023-31047**	https://www.djangoproject.com/weblog/2023/may/03/security-releases/, https://docs.djangoproject.com/en/4.2/releases/security/	A-DJA-DJAN-170523/87
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.19					
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation	https://www.djangoproject.com/weblog/2023/may/03/secur	A-DJA-DJAN-170523/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. **CVE ID : CVE-2023-31047**	ity-releases/, https://docs.djangoproject.com/en/4.2/releases/security/	
Affected Version(s): From (including) 4.0 Up to (excluding) 4.1.9					
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. **CVE ID : CVE-2023-31047**	https://www.djangoproject.com/weblog/2023/may/03/security-releases/, https://docs.djangoproject.com/en/4.2/releases/security/	A-DJA-DJAN-170523/89
Vendor: dmtf					
Product: libspdm					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.3.2					
Improper Authentication	08-May-2023	8.8	libspdm is a sample implementation that follows the DMTF SPDM specifications. A vulnerability has been identified in SPDM session establishment in libspdm prior to version 2.3.1. If a device supports both DHE session and PSK session with mutual authentication, the attacker may be able to establish the session with `KEY_EXCHANGE` and `PSK_FINISH` to bypass the mutual authentication. This is most likely to happen when the Requester begins a session using one method (DHE, for example) and then uses the other method's finish (PSK_FINISH in this example) to establish the session. The session hashes would be expected to fail in this case, but the condition was not detected. This issue only impacts the SPDM responder, which supports	https://github.com/DMTF/libspdm/security/advisories/GHSA-qw76-4v8p-xq9f, https://github.com/DMTF/libspdm/pull/2007, https://github.com/DMTF/libspdm/pull/2006	A-DMT-LIBS-170523/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`KEY_EX_CAP=1 and `PSK_CAP=10b` at same time with mutual authentication requirement. The SPDM requester is not impacted. The SPDM responder is not impacted if `KEY_EX_CAP=0` or `PSK_CAP=0` or `PSK_CAP=01b`. The SPDM responder is not impacted if mutual authentication is not required. libspdm 1.0, 2.0, 2.1, 2.2, 2.3 are all impacted. Older branches are not maintained, but users of the 2.3 branch may receive a patch in version 2.3.2. The SPDM specification (DSP0274) does not contain this vulnerability. **CVE ID : CVE-2023-31127**		
Vendor: douphp					
Product: douphp					
Affected Version(s): 1.7					
Improper Neutralization of Input During	03-May-2023	4.8	A stored cross-site scripting (XSS) vulnerability in DouPHP v1.7 allows attackers to execute	N/A	A-DOU-DOUP-170523/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			arbitrary web scripts or HTML via a crafted payload injected into the unique_id parameter in /admin/article.php. **CVE ID : CVE-2023-30205**		
Vendor: dreamer_cms_project					
Product: dreamer_cms					
Affected Version(s): * Up to (including) 4.1.3					
Inefficient Algorithmic Complexity	02-May-2023	7.5	A vulnerability was found in Dreamer CMS up to 4.1.3. It has been declared as problematic. This vulnerability affects the function updatePwd of the file UserController.java of the component Password Hash Calculation. The manipulation leads to inefficient algorithmic complexity. The attack can be initiated remotely. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-227860. **CVE ID : CVE-2023-2473**	N/A	A-DRE-DREA-170523/92
Vendor: e-office					
Product: e-office					
Affected Version(s): 9.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	04-May-2023	9.8	A vulnerability was found in Weaver E-Office 9.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file App/Ajax/ajax.php?action=mobile_upload_save. The manipulation of the argument upload_quwan leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228014 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2523**	N/A	A-E-O-E-OF-170523/93
Vendor: easytor					
Product: easytor					
Affected Version(s): *					
Authorization Bypass Through User-Controlled Key	08-May-2023	9.8	EasyTor Applications – Authorization Bypass - EasyTor Applications may allow authorization	N/A	A-EAS-EASY-170523/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass via unspecified method. **CVE ID : CVE-2023-31182**		
Vendor: easy_event_calendar_project					
Product: easy_event_calendar					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CoreFortress Easy Event calendar plugin <= 1.0 versions. **CVE ID : CVE-2023-28169**	N/A	A-EAS-EASY-170523/95
Vendor: echa.europa					
Product: iuclid					
Affected Version(s): From (including) 5.15.0 Up to (excluding) 6.27.6					
Use of Hard-coded Credentials	02-May-2023	9.8	European Chemicals Agency IUCLID 6.x before 6.27.6 allows authentication bypass because a weak hard-coded secret is used for JWT signing. The affected versions are 5.15.0 through 6.27.5. **CVE ID : CVE-2023-26089**	https://iuclid6.echa.europa.eu/documents/1387205/1809530/note_v6.27.6.pdf/76545a65-e6be-6486-280a-7d7c3d2ad455?t=1677577170669	A-ECH-IUCL-170523/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-May-2023	8.8	European Chemicals Agency IUCLID before 6.27.6 allows remote authenticated users to execute arbitrary code via Server Side Template Injection (SSTI) with a crafted template file. The attacker must have template manager permission. **CVE ID : CVE-2023-26546**	https://iuclid6.echa.europa.eu/documents/1387205/1809530/note_v6.27.6.pdf/76545a65-e6be-6486-280a-7d7c3d2ad455?t=1677577170669	A-ECH-IUCL-170523/97
Vendor: effectindex					
Product: tripreporter					
Affected Version(s): * Up to (excluding) 2023-04-30					
Improper Authentication	08-May-2023	9.1	`effectindex/tripreporter` is a community-powered, universal platform for submitting and analyzing trip reports. Prior to commit bd80ba833b9023d39ca22e29874296c8729dd53b, any user with an account on an instance of `effectindex/tripreporter`, e.g. `subjective.report`, may be affected by an improper password verification vulnerability. The vulnerability allows any user with a password matching	https://github.com/effectindex/tripreporter/security/advisories/GHSA-356r-rwp8-h6m6, https://github.com/effectindex/tripreporter/commit/bd80ba833b9023d39ca22e29874296c8729dd53b	A-EFF-TRIP-170523/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the password requirements to log in as any user. This allows access to accounts / data loss of the user. This issue is patched in commit bd80ba833b9023d39ca22e29874296c8729dd53b. No action necessary for users of `subjective.report`, and anyone running their own instance should update to this commit or newer as soon as possible. As a workaround, someone running their own instance may apply the patch manually. **CVE ID : CVE-2023-31123**		
Vendor: ejs					
Product: ejs					
Affected Version(s): 3.1.9					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-May-2023	9.8	ejs v3.1.9 is vulnerable to server-side template injection. If the ejs file is controllable, template injection can be implemented through the configuration settings of the closeDelimiter parameter. **CVE ID : CVE-2023-29827**	https://github.com/mde/ejs/issues/720	A-EJS-EJS-170523/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Elastic					
Product: filebeat					
Affected Version(s): * Up to (including) 7.17.9					
Insertion of Sensitive Information into Log File	04-May-2023	3.3	Filebeat versions through 7.17.9 and 8.6.2 have a flaw in httpjson input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled. **CVE ID : CVE-2023-31413**	https://www.elastic.co/community/security/, https://discuss.elastic.co/t/elastic-stack-8-7-0-7-17-10-security-updates/332327	A-ELA-FILE-170523/100
Affected Version(s): 8.6.2					
Insertion of Sensitive Information into Log File	04-May-2023	3.3	Filebeat versions through 7.17.9 and 8.6.2 have a flaw in httpjson input that allows the http request Authorization or Proxy-Authorization header contents to be leaked in the logs when debug logging is enabled. **CVE ID : CVE-2023-31413**	https://www.elastic.co/community/security/, https://discuss.elastic.co/t/elastic-stack-8-7-0-7-17-10-security-updates/332327	A-ELA-FILE-170523/101
Product: kibana					
Affected Version(s): 8.7.0					
Improper Control of Generation of Code ('Code Injection')	04-May-2023	8.8	Kibana version 8.7.0 contains an arbitrary code execution flaw. An attacker with All privileges to the Uptime/Synthetics feature could send a	https://www.elastic.co/community/security/, https://discuss.elastic.co/t/kibana-8-	A-ELA-KIBA-170523/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request that will attempt to execute JavaScript code. This could lead to the attacker executing arbitrary commands on the host system with permissions of the Kibana process. **CVE ID : CVE-2023-31415**	7-1-security-updates/332330	
Affected Version(s): From (including) 8.0.0 Up to (including) 8.7.0					
Improper Control of Generation of Code ('Code Injection')	04-May-2023	8.8	Kibana versions 8.0.0 through 8.7.0 contain an arbitrary code execution flaw. An attacker with write access to Kibana yaml or env configuration could add a specific payload that will attempt to execute JavaScript code. This could lead to the attacker executing arbitrary commands on the host system with permissions of the Kibana process. **CVE ID : CVE-2023-31414**	https://www.elastic.co/community/security/, https://discuss.elastic.co/t/kibana-8-7-1-security-updates/332330	A-ELA-KIBA-170523/103
Vendor: emqx					
Product: nanomq					
Affected Version(s): 0.15.0					
Out-of-bounds Write	04-May-2023	7.5	In NanoMQ v0.15.0-0, Heap overflow occurs in read_byte function of mqtt_code.c.	N/A	A-EMQ-NANO-170523/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29994		
Out-of-bounds Write	04-May-2023	7.5	In NanoMQ v0.15.0-0, a Heap overflow occurs in copyn_utf8_str function of mqtt_parser.c **CVE ID : CVE-2023-29995**	N/A	A-EMQ-NANO-170523/105
NULL Pointer Dereference	04-May-2023	7.5	In NanoMQ v0.15.0-0, segment fault with Null Pointer Dereference occurs in the process of decoding subinfo_decode and unsubinfo_decode. **CVE ID : CVE-2023-29996**	N/A	A-EMQ-NANO-170523/106
Vendor: enable\/disable_auto_login_when_register_project					
Product: enable\/disable_auto_login_when_register					
Affected Version(s): * Up to (including) 1.1.0					
Cross-Site Request Forgery (CSRF)	08-May-2023	6.5	The Enable/Disable Auto Login when Register WordPress plugin through 1.1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack **CVE ID : CVE-2023-0522**	N/A	A-ENA-ENAB-170523/107
Vendor: Enalean					
Product: tuleap					
Affected Version(s): From (including) 14.7.99.76 Up to (excluding) 14.7.99.143					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	Tuleap Open ALM is a Libre and Open Source tool for end to end traceability of application and system developments. The title of an artifact is not properly escaped in the tooltip. A malicious user with the capability to create an artifact or to edit a field title could force victim to execute uncontrolled code. This issue has been patched in version 14.7.99.143. **CVE ID : CVE-2023-30619**	https://github.com/Enalean/tuleap/security/advisories/GHSA-7fm3-cr3g-5922, https://tuleap.net/plugins/git/tuleap/tuleap/stable?a=commit&h=fdc93a736cbccad05de16ff0cc7cc3ef18dc93df, https://tuleap.net/plugins/tracker/?aid=31586	A-ENA-TULE-170523/108
Vendor: enhanced_wp_contact_form_project					
Product: enhanced_wp_contact_form					
Affected Version(s): * Up to (including) 2.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joost de Valk Enhanced WP Contact Form plugin <= 2.2.3 versions. **CVE ID : CVE-2023-23812**	N/A	A-ENH-ENHA-170523/109
Vendor: Esri					
Product: portal_for_arcgis					
Affected Version(s): 10.7.1					
Improper Neutralizat	09-May-2023	6.1	There is a reflected XSS vulnerability in	https://www.esri.com/a	A-ESR-PORT-170523/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID : CVE-2023-25830**	rcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2023-update-1-patch-is-now-available/	
Affected Version(s): 10.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID : CVE-2023-25830**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2023-update-1-patch-is-now-available/	A-ESR-PORT-170523/111
Affected Version(s): 10.9.1					
URL Redirection to Untrusted Site ('Open Redirect')	09-May-2023	6.1	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-	A-ESR-PORT-170523/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL that could redirect a victim to an arbitrary website, simplifying phishing attacks. **CVE ID : CVE-2023-25829**	arcgis-security-2023-update-1-patch-is-now-available/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1, 10.8.1 and 10.7.1 which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. **CVE ID : CVE-2023-25830**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2023-update-1-patch-is-now-available/	A-ESR-PORT-170523/113
Affected Version(s): 11.0					
URL Redirection to Untrusted Site ('Open Redirect')	09-May-2023	6.1	There is an unvalidated redirect vulnerability in Esri Portal for ArcGIS 11.0 and 10.9.1 that may allow a remote, unauthenticated attacker to craft a URL that could redirect a victim to an arbitrary website, simplifying phishing attacks. **CVE ID : CVE-2023-25829**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-security-2023-update-1-patch-is-now-available/	A-ESR-PORT-170523/114
Vendor: evasys					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: evasys					
Affected Version(s): 8.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	8.8	A SQL injection issue in Logbuch in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allows authenticated attackers to execute SQL statements via the welche parameter. **CVE ID : CVE-2023-31433**	N/A	A-EVA-EVAS-170523/115
Incorrect Authorization	02-May-2023	8.1	Multiple components (such as Onlinetemplate-Verwaltung, Liste aller Teilbereiche, Umfragen anzeigen, and questionnaire previews) in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allow authenticated attackers to read and write to unauthorized data by accessing functions directly. **CVE ID : CVE-2023-31435**	N/A	A-EVA-EVAS-170523/116
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The parameters nutzer_titel, nutzer_vn, and nutzer_nn in the user profile, and langID and ONLINEID in direct links, in evasys before 8.2 Build 2286 and 9.x before	N/A	A-EVA-EVAS-170523/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.0 Build 2401 do not validate input, which allows authenticated attackers to inject HTML Code and XSS payloads in multiple locations. **CVE ID : CVE-2023-31434**		
Affected Version(s): 9.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	8.8	A SQL injection issue in Logbuch in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allows authenticated attackers to execute SQL statements via the welche parameter. **CVE ID : CVE-2023-31433**	N/A	A-EVA-EVAS-170523/118
Incorrect Authorization	02-May-2023	8.1	Multiple components (such as Onlinetemplate-Verwaltung, Liste aller Teilbereiche, Umfragen anzeigen, and questionnaire previews) in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 allow authenticated attackers to read and write to unauthorized data by accessing functions directly. **CVE ID : CVE-2023-31435**	N/A	A-EVA-EVAS-170523/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The parameters nutzer_titel, nutzer_vn, and nutzer_nn in the user profile, and langID and ONLINEID in direct links, in evasys before 8.2 Build 2286 and 9.x before 9.0 Build 2401 do not validate input, which allows authenticated attackers to inject HTML Code and XSS payloads in multiple locations. **CVE ID : CVE-2023-31434**	N/A	A-EVA-EVAS-170523/120
Vendor: exquisite_paypal_donation_project					
Product: exquisite_paypal_donation					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in DgCult Exquisite PayPal Donation plugin <= v2.0.0 versions. **CVE ID : CVE-2023-23785**	N/A	A-EXQ-EXQU-170523/121
Vendor: eyes_only_user_access_shortcode_project					
Product: eyes_only_user_access_shortcode					
Affected Version(s): * Up to (including) 1.8.2					
Improper Neutralization of Input During Web Page	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Thom Stark Eyes Only: User Access	N/A	A-EYE-EYES-170523/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Shortcode plugin <= 1.8.2 versions. **CVE ID : CVE-2023-25786**		
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/123
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/125
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/127
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	A-F5-BIG--170523/129
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132539	A-F5-BIG--170523/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24461		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/131
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/133
Affected Version(s): From (including) 14.1.0 Up to (including) 14.1.5					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	A-F5-BIG--170523/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24461**	https://my.f5.com/manage/s/article/K000132539	A-F5-BIG--170523/135
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/136
Improper Limitation of a Pathname to a Restricted Directory	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/138
Affected Version(s): From (including) 15.1.0 Up to (including) 15.1.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	A-F5-BIG--170523/139
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24461**	https://my.f5.com/manage/s/article/K000132539	A-F5-BIG--170523/140
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/142
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (including) 16.1.3					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	A-F5-BIG--170523/144
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP	https://my.f5.com/manage/s/article/K000132539	A-F5-BIG--170523/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24461**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/146
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 17.0.0 Up to (including) 17.1.0					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	A-F5-BIG--170523/148
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note:	https://my.f5.com/manage/s/article/K000132539	A-F5-BIG--170523/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24461**		
Affected Version(s): From (including) 7.2.2 Up to (excluding) 7.2.4.1					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	A-F5-BIG--170523/150
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132539	A-F5-BIG--170523/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24461		
Product: big-ip_advanced_firewall_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/152
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/154
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/155
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/156
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/158
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/160
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/162
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/164
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/166
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/168
Product: big-ip_advanced_web_application_firewall					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/170
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/172
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/174
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/176
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/178
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/180
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/182
Improper Neutralization of Input	03-May-2023	6.1	Multiple reflected cross-site scripting	https://my.f5.com/mana	A-F5-BIG--170523/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	ge/s/article/K000132726	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28406		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/185
Product: big-ip_analytics					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/187
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/189
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/191
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/193
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/195
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/197
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/199
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/201
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Product: big-ip_application_acceleration_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/203
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/205
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/207
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/209
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/211
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/213
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/215
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/217
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27378		
Product: big-ip_application_security_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/220
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/222
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/223
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/224
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/226
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/228
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/230
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/232
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/234
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/236
Product: big-ip_application_visibility_and_reporting					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/238
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/240
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/242
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/244
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/246
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/248
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/250
Improper Neutralization of Input	03-May-2023	6.1	Multiple reflected cross-site scripting	https://my.f5.com/mana	A-F5-BIG--170523/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	ge/s/article/K000132726	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28406		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/253
Product: big-ip_carrier-grade_nat					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/255
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/257
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/259
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/261
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/263
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/265
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/267
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/269
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Product: big-ip_ddos_hybrid_defender					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/271
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/273
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/275
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/277
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/279
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/281
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/283
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/285
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27378		
Product: big-ip_domain_name_system					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/288
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/290
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/291
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28742**	https://my.f5.com/manage/s/article/K000132972	A-F5-BIG--170523/292
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/294
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh.	https://my.f5.com/manage/s/article/K000132972	A-F5-BIG--170523/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28742**		
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/296
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/298
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh.	https://my.f5.com/manage/s/article/K000132972	A-F5-BIG--170523/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28742**		
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/300
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/302
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Improper Neutralization of Special Elements used in an OS Command	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command execution	https://my.f5.com/manage/s/article/K000132972	A-F5-BIG--170523/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28742**		
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/304
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/306
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Neutralization of Special Elements	03-May-2023	8.8	When DNS is provisioned, an authenticated remote command	https://my.f5.com/manage/s/article/K000132972	A-F5-BIG--170523/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			execution vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28742**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28406		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/309
Product: big-ip_edge_gateway					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/311
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/313
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/315
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/317
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/319
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/321
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/323
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/325
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Product: big-ip_fraud_protection_service					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/327
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/329
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/331
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/333
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/335
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/337
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/339
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/341
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27378		
Product: big-ip_global_traffic_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/344
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/346
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/347
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/348
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/350
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/352
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/354
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/356
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/358
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/360
Product: big-ip_link_controller					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/362
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/364
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/366
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/368
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/370
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/372
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/374
Improper Neutralization of Input	03-May-2023	6.1	Multiple reflected cross-site scripting	https://my.f5.com/mana	A-F5-BIG--170523/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	ge/s/article/K000132726	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28406		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/377
Product: big-ip_local_traffic_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/379
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/381
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/383
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/385
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/387
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/389
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/391
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/393
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Product: big-ip_next_service_proxy_for_kubernetes					
Affected Version(s): 1.5.0					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/395
Product: big-ip_policy_enforcement_manager					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/397
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/399
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/401
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/403
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/405
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/407
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/409
Improper Neutralization of Input	03-May-2023	6.1	Multiple reflected cross-site scripting	https://my.f5.com/mana	A-F5-BIG--170523/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	ge/s/article/K000132726	
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28406		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/412
Product: big-ip_ssl_orchestrator					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/414
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/416
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/418
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/420
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/422
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/424
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/426
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/428
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Product: big-ip_webaccelerator					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/430
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/432
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note:	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/434
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/436
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/438
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server,	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/440
Improper Neutralization of Input During Web Page	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/442
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/444
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27378		
Product: big-ip_websafe					
Affected Version(s): 14.1.5					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/447
Affected Version(s): 15.1.4.1					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24594		
Affected Version(s): 16.1.2					
Uncontrolled Resource Consumption	03-May-2023	7.5	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24594**	https://my.f5.com/manage/s/article/K000133132	A-F5-BIG--170523/449
Affected Version(s): 17.0.0					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/450
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/451
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/453
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/455
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.8.2					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29163		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/457
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.4					
Missing Release of Memory after Effective Lifetime	03-May-2023	7.5	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29163**	https://my.f5.com/manage/s/article/K20145107	A-F5-BIG--170523/459
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained.	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/461
Affected Version(s): From (including) 17.0.0 Up to (excluding) 17.1.0.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	6.5	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not	https://my.f5.com/manage/s/article/K000132768	A-F5-BIG--170523/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28406**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-27378**	https://my.f5.com/manage/s/article/K000132726	A-F5-BIG--170523/463
Product: big-iq_centralized_management					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.3.0					
Unrestricted Upload of File with Dangerous Type	03-May-2023	5.4	An authenticated attacker granted a Viewer or Auditor role on a BIG-IQ can	https://my.f5.com/manage/s/article/K000132719	A-F5-BIG--170523/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload arbitrary files using an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-29240**		
Product: nginx_api_connectivity_manager					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.5.0					
Authorization Bypass Through User-Controlled Key	03-May-2023	8.1	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28656**	https://my.f5.com/manage/s/article/K000133417	A-F5-NGIN-170523/465
Incorrect Default	03-May-2023	7.1		https://my.f5.com/mana	A-F5-NGIN-170523/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28724**	ge/s/article/K000133233	
Product: nginx_instance_manager					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.9.0					
Authorization Bypass Through User-Controlled Key	03-May-2023	8.1	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of	https://my.f5.com/manage/s/article/K000133417	A-F5-NGIN-170523/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28656**		
Incorrect Default Permissions	03-May-2023	7.1	NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28724**	https://my.f5.com/manage/s/article/K000133233	A-F5-NGIN-170523/468
Product: nginx_security_monitoring					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	03-May-2023	8.1	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28656**	https://my.f5.com/manage/s/article/K000133417	A-F5-NGIN-170523/469
Incorrect Default Permissions	03-May-2023	7.1	NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have	https://my.f5.com/manage/s/article/K000133233	A-F5-NGIN-170523/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-28724**		
Vendor: fareharbor					
Product: fareharbor					
Affected Version(s): * Up to (excluding) 3.6.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in FareHarbor FareHarbor for WordPress plugin <= 3.6.6 versions. **CVE ID : CVE-2023-25021**	N/A	A-FAR-FARE-170523/471
Vendor: fastlinemedia					
Product: customizer_export\/import					
Affected Version(s): * Up to (excluding) 0.9.6					
Deserialization of Untrusted Data	08-May-2023	7.2	The Customizer Export/Import WordPress plugin before 0.9.6 unserializes user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present	N/A	A-FAS-CUST-170523/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1347		
Vendor: Fedoraproject					
Product: extra_packages_for_enterprise_linux					
Affected Version(s): 7.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. **CVE ID : CVE-2023-30944**	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77187	A-FED-EXTR-170523/473
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. **CVE ID : CVE-2023-30943**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77718, https://moodle.org/mod/forum/discuss.php?d=446285, https://bugzilla.redhat.com/show_bug.cgi?id=2188605	A-FED-EXTR-170523/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: finviz					
Product: stock_market_charts_from_finviz					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Moris Dov Stock market charts from finviz plugin <= 1.0.1 versions. **CVE ID : CVE-2023-23809**	N/A	A-FIN-STOC-170523/475
Vendor: firecask_like_\&_share_button_project					
Product: firecask_like_\&_share_button					
Affected Version(s): * Up to (including) 1.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Moss FireCask Like & Share Button plugin <= 1.1.5 versions. **CVE ID : CVE-2023-25783**	N/A	A-FIR-FIRE-170523/476
Vendor: food_ordering_management_system_project					
Product: food_ordering_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-May-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Food Ordering Management System 1.0. Affected is an unknown function of the component Registration. The manipulation of the	N/A	A-FOO-FOOD-170523/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-228396. **CVE ID : CVE-2023-2594**		
Vendor: Fortinet					
Product: fortiadc					
Affected Version(s): 7.2.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC 7.2.0, 7.1.0 through 7.1.1 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2023-27999**	https://fortiguard.com/psirt/FG-IR-22-297	A-FOR-FORT-170523/478
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	7.1	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file	https://fortiguard.com/psirt/FG-IR-23-069	A-FOR-FORT-170523/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system via crafted CLI commands. **CVE ID : CVE-2023-27993**		
Affected Version(s): From (including) 5.2.0 Up to (including) 7.0.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-May-2023	7.1	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file system via crafted CLI commands. **CVE ID : CVE-2023-27993**	https://fortiguard.com/psirt/FG-IR-23-069	A-FOR-FORT-170523/480
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.1.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	7.8	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC 7.2.0, 7.1.0 through 7.1.1 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands. **CVE ID : CVE-2023-27999**	https://fortiguard.com/psirt/FG-IR-22-297	A-FOR-FORT-170523/481
Improper Limitation of a Pathname	03-May-2023	7.1	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and	https://fortiguard.com/psirt/FG-IR-23-069	A-FOR-FORT-170523/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file system via crafted CLI commands. **CVE ID : CVE-2023-27993**		
Product: fortinac					
Affected Version(s): From (including) 8.7.0 Up to (excluding) 9.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	9	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses. **CVE ID : CVE-2023-22637**	https://fortiguard.com/psirt/FG-IR-23-013	A-FOR-FORT-170523/483
Affected Version(s): From (including) 8.7.0 Up to (including) 9.2.7					
Use of Hard-coded Credentials	03-May-2023	7.8	A use of hard-coded credentials vulnerability [CWE-798] in FortiNAC-F version 7.2.0, FortiNAC version	https://fortiguard.com/psirt/FG-IR-22-520	A-FOR-FORT-170523/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands. **CVE ID : CVE-2023-26203**		
Affected Version(s): From (including) 9.4.0 Up to (excluding) 9.4.3					
Use of Hard-coded Credentials	03-May-2023	7.8	A use of hard-coded credentials vulnerability [CWE-798] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands. **CVE ID : CVE-2023-26203**	https://fortiguard.com/psirt/FG-IR-22-520	A-FOR-FORT-170523/485
Product: fortinac-f					
Affected Version(s): 7.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	9	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2	https://fortiguard.com/psirt/FG-IR-23-013	A-FOR-FORT-170523/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses. **CVE ID : CVE-2023-22637**		
Use of Hard-coded Credentials	03-May-2023	7.8	A use of hard-coded credentials vulnerability [CWE-798] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands. **CVE ID : CVE-2023-26203**	https://fortiguard.com/psirt/FG-IR-22-520	A-FOR-FORT-170523/487
Product: fortiproxy					
Affected Version(s): 1.0.0					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13,	https://fortiguard.com/psirt/FG-IR-22-475	A-FOR-FORT-170523/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**		
Affected Version(s): 1.1.0					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2,	https://fortiguard.com/psirt/FG-IR-22-475	A-FOR-FORT-170523/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**		
Affected Version(s): 1.2.0					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.	https://fortiguard.com/psirt/FG-IR-22-475	A-FOR-FORT-170523/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22640		
Affected Version(s): 2.0.0					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**	https://fortiguard.com/psirt/FG-IR-22-475	A-FOR-FORT-170523/491
Vendor: fullworksplugins					
Product: quick_paypal_payments					
Affected Version(s): * Up to (excluding) 5.7.26.4					
Improper Neutralization of Input	02-May-2023	4.8	The Quick Paypal Payments WordPress plugin before 5.7.26.4 does	N/A	A-FUL-QUIC-170523/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-1554**		
Vendor: funadmin					
Product: funadmin					
Affected Version(s): * Up to (including) 3.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	A vulnerability was found in Funadmin up to 3.2.3. It has been declared as problematic. Affected by this vulnerability is the function tagLoad of the file Cx.php. The manipulation of the argument file 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-227869 was assigned to this vulnerability. **CVE ID : CVE-2023-2477**	N/A	A-FUN-FUNA-170523/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: geminilabs					
Product: site_reviews					
Affected Version(s): * Up to (excluding) 6.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	The Site Reviews WordPress plugin before 6.7.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-1525**	N/A	A-GEM-SITE-170523/494
Vendor: genomedics					
Product: millegpg					
Affected Version(s): 5.9.2					
Incorrect Permission Assignment for Critical Resource	04-May-2023	7.8	An issue was discovered in Genomedics MilleGP5 5.9.2, allows remote attackers to execute arbitrary code and gain escalated privileges via modifying specific files. **CVE ID : CVE-2023-25438**	https://millegpg.it/	A-GEN-MILL-170523/495
Vendor: Geovision					
Product: gv-edge_recording_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.2.3.0					
Incorrect Default Permissions	04-May-2023	9.8	An issue was discovered in GeoVision GV-Edge Recording Manager 2.2.3.0 for windows, which contains improper permissions within the default installation and allows attackers to execute arbitrary code and gain escalated privileges. **CVE ID : CVE-2023-23059**	N/A	A-GEO-GV-E-170523/496
Vendor: getrebuild					
Product: rebuild					
Affected Version(s): 3.2					
Cross-Site Request Forgery (CSRF)	02-May-2023	4.3	A vulnerability has been found in Rebuild 3.2 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-227866 is the identifier assigned to this vulnerability.	N/A	A-GET-REBU-170523/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2474		
Vendor: ghost					
Product: ghost					
Affected Version(s): * Up to (excluding) 5.42.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-May-2023	7.5	Ghost before 5.42.1 allows remote attackers to read arbitrary files within the active theme's folder via /assets/built%2F..%2F..%2F/ directory traversal. This occurs in frontend/web/middleware/static-theme.js. **CVE ID : CVE-2023-32235**	https://github.com/TryGhost/Ghost/commit/378dd913aa8d0fd0da29b0ffced8884579598b0f	A-GHO-GHOS-170523/498
Affected Version(s): * Up to (excluding) 5.46.1					
N/A	08-May-2023	7.5	Ghost is an app for new-media creators with tools to build a website, publish content, send newsletters, and offer paid subscriptions to members. Prior to version 5.46.1, due to a lack of validation when filtering on the public API endpoints, it is possible to reveal private fields via a brute force attack. Ghost(Pro) has already been	https://github.com/TryGhost/Ghost/security/advisories/GHSA-r97q-ghch-82j9, https://github.com/TryGhost/Ghost/commit/b3caf16005289cc9909488391b4a26f3f4a66a90	A-GHO-GHOS-170523/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched. Maintainers can find no evidence that the issue was exploited on Ghost(Pro) prior to the patch being added. Self-hosters are impacted if running Ghost a version below v5.46.1. v5.46.1 contains a fix for this issue. As a workaround, add a block for requests to `/ghost/api/content/*` where the `filter` query parameter contains `password` or `email`. **CVE ID : CVE-2023-31133**		
Vendor: gin-gonic					
Product: gin					
Affected Version(s): * Up to (excluding) 1.9.0					
Improper Input Validation	04-May-2023	9.8	Versions of the package github.com/gin-gonic/gin before 1.9.0 are vulnerable to Improper Input Validation by allowing an attacker to use a specially crafted request via the X-Forwarded-Prefix header, potentially leading to cache poisoning. **Note:** Although this issue does not	https://github.com/t0rchwo0d/gin/commit/fd9f98e70fb4107ee68c783482d231d35e60507b, https://github.com/gin-gonic/gin/pull/3500, https://security.snyk.io/vuln/SNYK-GOLANG-GITHUBCOM	A-GIN-GIN-170523/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pose a significant threat on its own it can serve as an input vector for other more impactful vulnerabilities. However, successful exploitation may depend on the server configuration and whether the header is used in the application logic. **CVE ID : CVE-2023-26125**	GINGONICGIN-3324285, https://github.com/gin-gonic/gin/pull/3503	
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): * Up to (excluding) 15.8.5					
URL Redirection to Untrusted Site ('Open Redirect')	03-May-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown **CVE ID : CVE-2023-0155**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0155.json	A-GIT-GITL-170523/501
Affected Version(s): * Up to (excluding) 15.9.6					
N/A	03-May-2023	8	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0756.json	A-GIT-GITL-170523/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems. **CVE ID : CVE-2023-0756**		
Affected Version(s): 15.11.0					
N/A	03-May-2023	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Under certain conditions when OpenID Connect is enabled on an instance, it may allow users who are marked as 'external' to become 'regular' users thus leading to privilege escalation for those users. **CVE ID : CVE-2023-2182**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2182.json, https://gitlab.com/gitlab-org/gitlab/-/issues/403012	A-GIT-GITL-170523/503
Affected Version(s): From (including) 10.0 Up to (excluding) 12.9.8					
N/A	03-May-2023	4.3	An issue has been discovered in GitLab	https://gitlab.com/gitlab	A-GIT-GITL-170523/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings. **CVE ID : CVE-2023-1204**	-org/cves/-/blob/master/2023/CVE-2023-1204.json	
Exposure of Resource to Wrong Sphere	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user with the role of developer could use the import project feature to leak CI/CD variables. **CVE ID : CVE-2023-2069**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2069.json	A-GIT-GITL-170523/505
Affected Version(s): From (including) 11.9 Up to (excluding) 15.9.6					
Session Fixation	03-May-2023	4.5	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1265.json	A-GIT-GITL-170523/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from all users of a GitLab instance. **CVE ID : CVE-2023-1265**		
Affected Version(s): From (including) 12.10 Up to (excluding) 12.10.7					
N/A	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings. **CVE ID : CVE-2023-1204**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1204.json	A-GIT-GITL-170523/507
Affected Version(s): From (including) 12.10.0 Up to (excluding) 12.10.7					
Exposure of Resource to Wrong Sphere	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2069.json	A-GIT-GITL-170523/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 13.0.1. A user with the role of developer could use the import project feature to leak CI/CD variables. **CVE ID : CVE-2023-2069**		
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0.1					
N/A	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user could use an unverified email as a public email and commit email by sending a specifically crafted request on user update settings. **CVE ID : CVE-2023-1204**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1204.json	A-GIT-GITL-170523/509
Exposure of Resource to Wrong Sphere	03-May-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 10.0 before 12.9.8, all versions starting from 12.10 before 12.10.7, all versions starting from 13.0 before 13.0.1. A user with the role of developer could use the import project	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2069.json	A-GIT-GITL-170523/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature to leak CI/CD variables. **CVE ID : CVE-2023-2069**		
Affected Version(s): From (including) 13.11 Up to (excluding) 15.8.5					
Exposure of Resource to Wrong Sphere	03-May-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user role to read project updates by doing a diff with a pre-existing fork. **CVE ID : CVE-2023-0485**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0485.json	A-GIT-GITL-170523/511
Affected Version(s): From (including) 14.2 Up to (excluding) 15.9.6					
Cross-Site Request Forgery (CSRF)	03-May-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1965.json	A-GIT-GITL-170523/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3rd party Group SAML SSO logins. This feature isn't enabled by default. **CVE ID : CVE-2023-1965**		
Affected Version(s): From (including) 15.10 Up to (excluding) 15.10.1					
URL Redirection to Untrusted Site ('Open Redirect')	03-May-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown **CVE ID : CVE-2023-0155**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0155.json	A-GIT-GITL-170523/513
Affected Version(s): From (including) 15.10 Up to (excluding) 15.10.5					
N/A	03-May-2023	8.1	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public group even after being banned from the public group by the owner.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0805.json	A-GIT-GITL-170523/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0805		
N/A	03-May-2023	8	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems. **CVE ID : CVE-2023-0756**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0756.json	A-GIT-GITL-170523/515
Cross-Site Request Forgery (CSRF)	03-May-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1965.json	A-GIT-GITL-170523/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3rd party Group SAML SSO logins. This feature isn't enabled by default. **CVE ID : CVE-2023-1965**		
Improper Control of Generation of Code ('Code Injection')	03-May-2023	5.7	An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages are pulled from a tag or from a release containing a ref to another commit. **CVE ID : CVE-2023-1178**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1178.json	A-GIT-GITL-170523/517
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1836.json	A-GIT-GITL-170523/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			under specific circumstances **CVE ID : CVE-2023-1836**		
Session Fixation	03-May-2023	4.5	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from all users of a GitLab instance. **CVE ID : CVE-2023-1265**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1265.json	A-GIT-GITL-170523/519
Affected Version(s): From (including) 15.10.0 Up to (excluding) 15.10.5					
N/A	03-May-2023	8.8	An issue has been discovered in GitLab EE affecting all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Under certain conditions when OpenID Connect is enabled on an instance, it may allow users who are marked as 'external' to become 'regular' users thus leading to	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2182.json, https://gitlab.com/gitlab-org/gitlab/-/issues/403012	A-GIT-GITL-170523/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege escalation for those users. **CVE ID : CVE-2023-2182**		
Affected Version(s): From (including) 15.10.0 Up to (excluding) 15.10.6					
Incorrect Permission Assignment for Critical Resource	08-May-2023	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project. **CVE ID : CVE-2023-2478**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2478.json	A-GIT-GITL-170523/521
Affected Version(s): From (including) 15.11 Up to (excluding) 15.11.1					
N/A	03-May-2023	8.1	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0805.json	A-GIT-GITL-170523/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			group even after being banned from the public group by the owner. **CVE ID : CVE-2023-0805**		
N/A	03-May-2023	8	An issue has been discovered in GitLab affecting all versions before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The main branch of a repository with a specially crafted name allows an attacker to create repositories with malicious code, victims who clone or download these repositories will execute arbitrary code on their systems. **CVE ID : CVE-2023-0756**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0756.json	A-GIT-GITL-170523/523
Exposure of Resource to Wrong Sphere	03-May-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0485.json	A-GIT-GITL-170523/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			role to read project updates by doing a diff with a pre-existing fork. **CVE ID : CVE-2023-0485**		
Cross-Site Request Forgery (CSRF)	03-May-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 14.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. Lack of verification on RelayState parameter allowed a maliciously crafted URL to obtain access tokens granted for 3rd party Group SAML SSO logins. This feature isn't enabled by default. **CVE ID : CVE-2023-1965**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1965.json	A-GIT-GITL-170523/525
Improper Control of Generation of Code ('Code Injection')	03-May-2023	5.7	An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1178.json	A-GIT-GITL-170523/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are pulled from a tag or from a release containing a ref to another commit. **CVE ID : CVE-2023-1178**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed under specific circumstances **CVE ID : CVE-2023-1836**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1836.json	A-GIT-GITL-170523/527
Session Fixation	03-May-2023	4.5	An issue has been discovered in GitLab affecting all versions starting from 11.9 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. The condition allows for a privileged attacker, under certain conditions, to obtain session tokens from	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1265.json	A-GIT-GITL-170523/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all users of a GitLab instance. **CVE ID : CVE-2023-1265**		
Affected Version(s): From (including) 15.11.0 Up to (excluding) 15.11.2					
Incorrect Permission Assignment for Critical Resource	08-May-2023	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project. **CVE ID : CVE-2023-2478**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2478.json	A-GIT-GITL-170523/529
Affected Version(s): From (including) 15.2 Up to (excluding) 15.9.6					
N/A	03-May-2023	8.1	An issue has been discovered in GitLab EE affecting all versions starting from 15.2 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. A malicious group member may continue to have access to the public projects of a public	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0805.json	A-GIT-GITL-170523/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			group even after being banned from the public group by the owner. **CVE ID : CVE-2023-0805**		
Affected Version(s): From (including) 15.4.0 Up to (excluding) 15.9.7					
Incorrect Permission Assignment for Critical Resource	08-May-2023	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.9.7, all versions starting from 15.10 before 15.10.6, all versions starting from 15.11 before 15.11.2. Under certain conditions, a malicious unauthorized GitLab user may use a GraphQL endpoint to attach a malicious runner to any project. **CVE ID : CVE-2023-2478**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2478.json	A-GIT-GITL-170523/531
Affected Version(s): From (including) 15.9 Up to (excluding) 15.9.4					
Exposure of Resource to Wrong Sphere	03-May-2023	6.5	An issue has been discovered in GitLab affecting all versions starting from 13.11 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible that a project member demoted to a user	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0485.json	A-GIT-GITL-170523/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			role to read project updates by doing a diff with a pre-existing fork. **CVE ID : CVE-2023-0485**		
Affected Version(s): From (including) 15.9 Up to (excluding) 15.9.5					
URL Redirection to Untrusted Site ('Open Redirect')	03-May-2023	5.4	An issue has been discovered in GitLab CE/EE affecting all versions before 15.8.5, 15.9.4, 15.10.1. Open redirects was possible due to framing arbitrary content on any page allowing user controlled markdown **CVE ID : CVE-2023-0155**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0155.json	A-GIT-GITL-170523/533
Affected Version(s): From (including) 5.1 Up to (excluding) 15.9.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 5.1 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. When viewing an XML file in a repository in "raw" mode, it can be made to render as HTML if viewed under specific circumstances	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1836.json	A-GIT-GITL-170523/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1836		
Affected Version(s): From (including) 8.6.0 Up to (excluding) 15.9.6					
Improper Control of Generation of Code ('Code Injection')	03-May-2023	5.7	An issue has been discovered in GitLab CE/EE affecting all versions from 8.6 before 15.9.6, all versions starting from 15.10 before 15.10.5, all versions starting from 15.11 before 15.11.1. File integrity may be compromised when source code or installation packages are pulled from a tag or from a release containing a ref to another commit. **CVE ID : CVE-2023-1178**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1178.json	A-GIT-GITL-170523/535
Vendor: givewp					
Product: givewp					
Affected Version(s): * Up to (excluding) 2.25.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in GiveWP plugin <= 2.25.1 versions. **CVE ID : CVE-2023-23668**	N/A	A-GIV-GIVE-170523/536
Vendor: gmo					
Product: typesquare_webfonts_for_conoha					
Affected Version(s): * Up to (excluding) 2.0.4					
Improper Neutralizat	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site	N/A	A-GMO-TYPE-170523/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability in GMO Internet Group, Inc. TypeSquare Webfonts for ConoHa plugin <= 2.0.3 versions. **CVE ID : CVE-2023-25458**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 113.0.5672.63					
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2023-2461**	N/A	A-GOO-CHRO-170523/538
Improper Input Validation	03-May-2023	7.1	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted	N/A	A-GOO-CHRO-170523/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2460**		
N/A	03-May-2023	6.5	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2459**	N/A	A-GOO-CHRO-170523/540
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2462**	N/A	A-GOO-CHRO-170523/541
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar)	N/A	A-GOO-CHRO-170523/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2463**		
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2464**	N/A	A-GOO-CHRO-170523/543
N/A	03-May-2023	4.3	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2465**	N/A	A-GOO-CHRO-170523/544
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote	N/A	A-GOO-CHRO-170523/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2466**		
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2467**	N/A	A-GOO-CHRO-170523/546
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2468**	N/A	A-GOO-CHRO-170523/547
Product: web_stories					
Affected Version(s): * Up to (excluding) 1.32.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	08-May-2023	6.5	The Web Stories for WordPress plugin supports the WordPress built-in functionality of protecting content with a password. The content is then only accessible to website visitors after entering the password. In WordPress, users with the "Author" role can create stories, but don't have the ability to edit password protected stories. The vulnerability allowed users with said role to bypass this permission check when trying to duplicate the protected story in the plugin's own dashboard, giving them access to the seemingly protected content. We recommend upgrading to version 1.32 or beyond commit ad49781c2a35c5c92ef704d4b621ab4e5cb77d68 https://github.com/GoogleForCreators/web-stories-wp/commit/ad49781c2a35c5c92ef704d4b621ab4e5cb77d68	https://github.com/GoogleForCreators/web-stories-wp/commit/ad49781c2a35c5c92ef704d4b621ab4e5cb77d68	A-GOO-WEB_-170523/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1979		
Vendor: greentreelabs					
Product: circles_gallery					
Affected Version(s): * Up to (including) 1.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GreenTreeLabs Circles Gallery plugin <= 1.0.10 versions. **CVE ID : CVE-2023-23881**	N/A	A-GRE-CIRC-170523/549
Vendor: hashicorp					
Product: vault					
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.2					
Inadequate Encryption Strength	01-May-2023	2.5	HashiCorp Vault Enterprise 1.13.0 up to 1.13.1 is vulnerable to a padding oracle attack when using an HSM in conjunction with the CKM_AES_CBC_PAD or CKM_AES_CBC encryption mechanisms. An attacker with privileges to modify storage and restart Vault may be able to intercept or modify cipher text in order to derive Vault's root key. Fixed in 1.13.2 **CVE ID : CVE-2023-2197**	https://discuss.hashicorp.com/t/hcsec-2023-14-vault-enterprise-vulnerable-to-padding-oracle-attacks-when-using-a-cbc-based-encryption-mechanism-with-a-hsm/53322	A-HAS-VAUL-170523/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: hu-manity					
Product: cookie_notice_\&_compliance_for_gdpr_\/_ccpa					
Affected Version(s): * Up to (excluding) 2.4.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-May-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Hu-manity.Co Cookie Notice & Compliance for GDPR / CCPA plugin <= 2.4.6 versions. **CVE ID : CVE-2023-24400**	N/A	A-HU--COOK-170523/551
Vendor: IBM					
Product: business_automation_workflow					
Affected Version(s): 18.0.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 18.0.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/553
Affected Version(s): 18.0.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**		
Affected Version(s): 20.0.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/555
Affected Version(s): 20.0.0.2					
Improper Neutralization of Input During Web Page	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1,	https://www.ibm.com/support/pages/node/6965776, https://exch	A-IBM-BUSI-170523/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	ange.xforce.ibmcloud.com/vulnerabilities/246115	
Affected Version(s): 21.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115.	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24957		
Affected Version(s): 22.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/558
Affected Version(s): 22.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**		
Affected Version(s): From (including) 19.0.0.1 Up to (including) 19.0.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/560
Affected Version(s): From (including) 20.0.0.1 Up to (excluding) 21.0.3					
Improper Neutralization of	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0,	https://www.ibm.com/support/page	A-IBM-BUSI-170523/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	s/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	
Affected Version(s): From (including) 21.0.1 Up to (including) 21.0.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**		
Affected Version(s): From (including) 22.0.1 Up to (excluding) 22.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	5.4	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, 19.0.0.3, 20.0.0.1, 20.0.0.2, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 246115. **CVE ID : CVE-2023-24957**	https://www.ibm.com/support/pages/node/6965776, https://exchange.xforce.ibmcloud.com/vulnerabilities/246115	A-IBM-BUSI-170523/563
Product: cloudant					
Affected Version(s): * Up to (including) 8349					
N/A	02-May-2023	5.3	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when	https://docs.couchdb.org/en/stable/cve/2023-26268.html	A-IBM-CLOU-170523/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using these design document functions: * validate_doc_update * list * filter * filter views (using view functions as filters) * rewrite * update This doesn't affect map/reduce or search (Dreyfus) index functions. Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3). Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data in the Javascript environment. **CVE ID : CVE-2023-26268**		
Product: elastic_storage_system					
Affected Version(s): From (including) 6.1.0.0 Up to (excluding) 6.1.2.6					
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X-Force ID: 252187. **CVE ID : CVE-2023-30434**	https://www.ibm.com/support/pages/node/6988365, https://www.ibm.com/support/pages/node/6988363, https://exchange.xforce.ibmcloud.com/vulnerabilities/252187	A-IBM-ELAS-170523/565
Affected Version(s): From (including) 6.1.3.0 Up to (excluding) 6.1.6.1					
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X-Force ID: 252187. **CVE ID : CVE-2023-30434**	https://www.ibm.com/support/pages/node/6988365, https://www.ibm.com/support/pages/node/6988363, https://exchange.xforce.ibmcloud.com/vulnerabilities/252187	A-IBM-ELAS-170523/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mq_appliance					
Affected Version(s): From (including) 9.2.0.0 Up to (excluding) 9.2.0.11					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X-Force ID: 248418. **CVE ID : CVE-2023-26285**	https://www.ibm.com/support/pages/node/6986563, https://exchange.xforce.ibmcloud.com/vulnerabilities/248418	A-IBM-MQ_A-170523/567
Affected Version(s): From (including) 9.2.0.0 Up to (excluding) 9.2.5.7					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X-Force ID: 248418. **CVE ID : CVE-2023-26285**	https://www.ibm.com/support/pages/node/6986563, https://exchange.xforce.ibmcloud.com/vulnerabilities/248418	A-IBM-MQ_A-170523/568
Affected Version(s): From (including) 9.2.0.0 Up to (excluding) 9.3.2					
Uncontrolled Resource Consumption	05-May-2023	5.5	IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files. IBM X-Force ID: 244216. **CVE ID : CVE-2023-22874**	https://www.ibm.com/support/pages/node/6985901, https://exchange.xforce.ibmcloud.com/vulnerabilities/244216	A-IBM-MQ_A-170523/569
Affected Version(s): From (including) 9.3.0.0 Up to (excluding) 9.3.0.5					
Improper Restriction	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3	https://www.ibm.com/s	A-IBM-MQ_A-170523/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X-Force ID: 248418. **CVE ID : CVE-2023-26285**	upport/pages/node/6986563, https://exchange.xforce.ibmcloud.com/vulnerabilities/248418	
Uncontrolled Resource Consumption	05-May-2023	5.5	IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files. IBM X-Force ID: 244216. **CVE ID : CVE-2023-22874**	https://www.ibm.com/support/pages/node/6985901, https://exchange.xforce.ibmcloud.com/vulnerabilities/244216	A-IBM-MQ_A-170523/571
Affected Version(s): From (including) 9.3.0.0 Up to (excluding) 9.3.2.1					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	7.5	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X-Force ID: 248418. **CVE ID : CVE-2023-26285**	https://www.ibm.com/support/pages/node/6986563, https://exchange.xforce.ibmcloud.com/vulnerabilities/248418	A-IBM-MQ_A-170523/572
Product: spectrum_scale					
Affected Version(s): From (including) 5.1.0.0 Up to (including) 5.1.2.9					
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0	https://www.ibm.com/support/pages/node/6988365, https://www.ibm.com/s	A-IBM-SPEC-170523/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X-Force ID: 252187. **CVE ID : CVE-2023-30434**	upport/pages/node/6988363, https://exchange.xforce.ibmcloud.com/vulnerabilities/252187	
Affected Version(s): From (including) 5.1.3.0 Up to (including) 5.1.6.1					
Improper Input Validation	05-May-2023	5.5	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X-Force ID: 252187. **CVE ID : CVE-2023-30434**	https://www.ibm.com/support/pages/node/6988365, https://www.ibm.com/support/pages/node/6988363, https://exchange.xforce.ibmcloud.com/vulnerabilities/252187	A-IBM-SPEC-170523/574
Vendor: Illumos					
Product: illumos-gate					
Affected Version(s): * Up to (excluding) 2023-04-29					
Out-of-bounds Write	04-May-2023	7.8	illumos illumos-gate before 676abcb has a stack buffer overflow in /dev/net, leading to privilege escalation via a stat on a long file name in /dev/net. **CVE ID : CVE-2023-31284**	N/A	A-ILL-ILLU-170523/575
Vendor: ipandao					
Product: editor.md					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	6.1	Cross Site Scripting (XSS) vulnerability in pandao editor.md thru 1.5.0 allows attackers to inject arbitrary web script or HTML via crafted markdown text. **CVE ID : CVE-2023-29641**	https://github.com/pandao/editor.md/issues/985	A-IPA-EDIT-170523/576
Vendor: j2eefast					
Product: j2eefast					
Affected Version(s): * Up to (including) 2.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	A vulnerability was found in Dromara J2eeFAST up to 2.6.0 and classified as problematic. This issue affects some unknown processing of the component System Message Handler. The manipulation of the argument ?? leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 7a9e1a00e3329fdc0ae05f7a8257cce77037134d. It is recommended to apply a patch to fix this issue. The associated identifier	N/A	A-J2E-J2EE-170523/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-227867. **CVE ID : CVE-2023-2475**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	A vulnerability was found in Dromara J2eeFAST up to 2.6.0. It has been classified as problematic. Affected is an unknown function of the component Announcement Handler. The manipulation of the argument ????/???? 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 name of the patch is 7a9e1a00e3329fdc0ae05f7a8257cce77037134d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-227868. **CVE ID : CVE-2023-2476**	N/A	A-J2E-J2EE-170523/578
Vendor: jch_optimize_project					
Product: jch_optimize					
Affected Version(s): * Up to (excluding) 3.2.3					
Improper Neutralization of	06-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-JCH-JCH_-170523/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Samuel Marshall JCH Optimize plugin <= 3.2.2 versions. **CVE ID : CVE-2023-25491**		
Vendor: jsreport					
Product: jsreport					
Affected Version(s): * Up to (excluding) 3.11.3					
Improper Control of Generation of Code ('Code Injection')	08-May-2023	10	Code Injection in GitHub repository jsreport/jsreport prior to 3.11.3. **CVE ID : CVE-2023-2583**	https://github.com/jsreport/jsreport/commit/afaff3804b34b38e959f5ae65f9e672088de13d7, https://huntr.dev/bounties/397ea68d-1e28-44ff-b830-c8883d067d96	A-JSR-JSRE-170523/580
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')	08-May-2023	9.8	Judging Management System v1.0 is vulnerable to SQL Injection. via /php-jms/review_se_result.php?mainevent_id=. **CVE ID : CVE-2023-30018**	N/A	A-JUD-JUDG-170523/581
Improper Neutralization of	04-May-2023	9.8	Judging Management System v1.0 by oretnom23 was	N/A	A-JUD-JUDG-170523/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			discovered to vulnerable to SQL injection via /php-jms/review_result.php?mainevent_id=, mainevent_id. **CVE ID : CVE-2023-30077**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the event_id parameter at /php-jms/result_sheet.php. **CVE ID : CVE-2023-30203**	N/A	A-JUD-JUDG-170523/583
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-May-2023	9.8	Judging Management System v1.0 was discovered to contain a SQL injection vulnerability via the judge_id parameter at /php-jms/edit_judge.php. **CVE ID : CVE-2023-30204**	N/A	A-JUD-JUDG-170523/584
Vendor: kanbanwp					
Product: kanban_boards_for_wordpress					
Affected Version(s): * Up to (including) 2.5.20					
Improper Neutralization of Input During Web Page Generation	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kanban for WordPress Kanban Boards for	N/A	A-KAN-KANB-170523/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			WordPress plugin <= 2.5.20 versions. **CVE ID : CVE-2023-23884**		
Vendor: konga_project					
Product: konga					
Affected Version(s): 0.14.9					
N/A	01-May-2023	6.5	An issue discovered in Konga 0.14.9 allows remote attackers to manipulate user accounts regardless of privilege via crafted POST request. **CVE ID : CVE-2023-26987**	N/A	A-KON-KONG-170523/586
Vendor: lazy_social_comments_project					
Product: lazy_social_comments					
Affected Version(s): * Up to (including) 2.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Joel James Lazy Social Comments plugin <= 2.0.4 versions. **CVE ID : CVE-2023-23733**	N/A	A-LAZ-LAZY-170523/587
Vendor: Libming					
Product: libming					
Affected Version(s): 0.4.8					
Buffer Copy without Checking Size of Input	09-May-2023	5.5	Buffer Overflow vulnerability found in Libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via	N/A	A-LIB-LIBM-170523/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			the newVar_N in util/decompile.c. **CVE ID : CVE-2023-30083**		
Out-of-bounds Read	09-May-2023	5.5	An issue found in libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the stackVal function in util/decompile.c. **CVE ID : CVE-2023-30084**	N/A	A-LIB-LIBM-170523/589
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-May-2023	5.5	Buffer Overflow vulnerability found in Libming swftophp v.0.4.8 allows a local attacker to cause a denial of service via the cws2fws function in util/decompile.c. **CVE ID : CVE-2023-30085**	N/A	A-LIB-LIBM-170523/590
Vendor: lightspeedhq					
Product: ecwid_ecommerce_shopping_cart					
Affected Version(s): * Up to (excluding) 6.11.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Ecwid Ecommerce Ecwid Ecommerce Shopping Cart plugin <= 6.11.4 versions. **CVE ID : CVE-2023-24408**	N/A	A-LIG-ECWI-170523/591
Vendor: limit_login_attempts_project					
Product: limit_login_attempts					
Affected Version(s): * Up to (including) 1.7.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.4	The Limit Login Attempts WordPress plugin through 1.7.2 does not sanitize and escape usernames when outputting them back in the logs dashboard, which could allow any authenticated users, such as subscriber to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-1861**	N/A	A-LIM-LIMI-170523/592
Vendor: Linuxfoundation					
Product: fluid					
Affected Version(s): From (including) 0.7.0 Up to (excluding) 0.8.6					
Incorrect Authorization	08-May-2023	7.8	Fluid is an open source Kubernetes-native distributed dataset orchestrator and accelerator for data-intensive applications. Starting in version 0.7.0 and prior to version 0.8.6, if a malicious user gains control of a Kubernetes node running fluid csi pod (controlled by the `csi-nodeplugin-fluid` node-daemonset), they can leverage the fluid-csi service account to modify specs of all the nodes in the cluster. However, since this service	https://github.com/fluid-cloudnative/fluid/commit/91c05c32db131997b5ca065e869c9918a125c149, https://github.com/fluid-cloudnative/fluid/commit/77c8110a3d1ec077ae2bce6bd88d296505db1550	A-LIN-FLUI-170523/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account lacks `list node` permissions, the attacker may need to use other techniques to identify vulnerable nodes. Once the attacker identifies and modifies the node specs, they can manipulate system-level-privileged components to access all secrets in the cluster or execute pods on other nodes. This allows them to elevate privileges beyond the compromised node and potentially gain full privileged access to the whole cluster. To exploit this vulnerability, the attacker can make all other nodes unschedulable (for example, patch node with taints) and wait for system-critical components with high privilege to appear on the compromised node. However, this attack requires two prerequisites: a compromised node		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and identifying all vulnerable nodes through other means. Version 0.8.6 contains a patch for this issue. As a workaround, delete the `csi-nodeplugin-fluid` daemonset in `fluid-system` namespace and avoid using CSI mode to mount FUSE file systems. Alternatively, using sidecar mode to mount FUSE file systems is recommended. **CVE ID : CVE-2023-30840**		
Product: rekor					
Affected Version(s): * Up to (excluding) 1.1.1					
Allocation of Resources Without Limits or Throttling	08-May-2023	7.5	Rekor is an open source software supply chain transparency log. Rekor prior to version 1.1.1 may crash due to out of memory (OOM) conditions caused by reading archive metadata files into memory without checking their sizes first. Verification of a JAR file submitted to Rekor can cause an out of memory crash	https://github.com/sigstore/rekor/commit/cf42ace82667025fe128f7a50cf6b4cdff51cc48, https://github.com/sigstore/rekor/security/advisories/GHSA-2h5h-59f5-c5x9	A-LIN-REKO-170523/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if files within the META-INF directory of the JAR are sufficiently large. Parsing of an APK file submitted to Rekor can cause an out of memory crash if the .SIGN or .PKGINFO files within the APK are sufficiently large. The OOM crash has been patched in Rekor version 1.1.1. There are no known workarounds. **CVE ID : CVE-2023-30551**		
Vendor: Llvm					
Product: llvm					
Affected Version(s): 2022-11-01					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-May-2023	5.5	llvm-project commit fdbc55a5 was discovered to contain a segmentation fault via the component mlir::IROperand<mlir::OpOperand. **CVE ID : CVE-2023-29932**	https://github.com/llvm/llvm-project/issues/58745	A-LLV-LLVM-170523/595
Affected Version(s): 2022-11-22					
Out-of-bounds Read	05-May-2023	5.5	llvm-project commit 6c01b5c was discovered to contain a segmentation fault via the component mlir::Type::getDialect().	https://github.com/llvm/llvm-project/issues/59136	A-LLV-LLVM-170523/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29934		
Affected Version(s): 2022-11-23					
Reachable Assertion	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain an assertion failure at !replacements.count(op) && "operation was already replaced. **CVE ID : CVE-2023-29935**	https://github.com/llvm/llvm-project/issues/59182	A-LLV-LLVM-170523/597
Affected Version(s): 2022-12-11					
Out-of-bounds Read	05-May-2023	5.5	llvm-project commit bd456297 was discovered to contain a segmentation fault via the component mlir::Block::getArgument. **CVE ID : CVE-2023-29933**	https://github.com/llvm/llvm-project/issues/59442	A-LLV-LLVM-170523/598
Affected Version(s): 2023-01-12					
Out-of-bounds Read	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::spirv::TargetEnv::TargetEnv(mlir::spirv::TargetEnvAttr). **CVE ID : CVE-2023-29939**	https://github.com/llvm/llvm-project/issues/59983	A-LLV-LLVM-170523/599
Out-of-bounds Read	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain a	https://github.com/llvm/llvm-	A-LLV-LLVM-170523/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			segmentation fault via the component matchAndRewriteSortOp<mlir::sparse_tensor::SortOp>(mlir::sparse_tensor::SortOp . **CVE ID : CVE-2023-29941**	project/issues/59988	
Out-of-bounds Read	05-May-2023	5.5	llvm-project commit a0138390 was discovered to contain a segmentation fault via the component mlir::Type::isa<mlir::LLVM::LLVMVoidType. **CVE ID : CVE-2023-29942**	https://github.com/llvm/llvm-project/issues/59990	A-LLV-LLVM-170523/601
Vendor: machothemes					
Product: newsmag					
Affected Version(s): * Up to (including) 2.4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Auth (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Macho Themes NewsMag theme <= 2.4.4 versions. **CVE ID : CVE-2023-28493**	N/A	A-MAC-NEWS-170523/602
Vendor: mailbutler					
Product: shimo					
Affected Version(s): 5.0.4					
Improper Authentication	04-May-2023	9.8	An issue in the helper tool of Mailbutler GmbH Shimo VPN Client for macOS v5.0.4 allows	N/A	A-MAI-SHIM-170523/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to bypass authentication via PID re-use. **CVE ID : CVE-2023-30328**		
Vendor: mattermost					
Product: mattermost_desktop					
Affected Version(s): * Up to (including) 5.2.2					
URL Redirection to Untrusted Site ('Open Redirect')	02-May-2023	5.4	Mattermost Desktop App fails to validate a mattermost server redirection and navigates to an arbitrary website **CVE ID : CVE-2023-2000**	https://mattermost.com/security-updates	A-MAT-MATT-170523/604
Vendor: metaphorcreations					
Product: ditty					
Affected Version(s): * Up to (excluding) 3.0.33					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Metaphor Creations Ditty plugin <= 3.0.32 versions. **CVE ID : CVE-2023-23874**	N/A	A-MET-DITT-170523/605
Vendor: metersphere					
Product: metersphere					
Affected Version(s): * Up to (excluding) 2.9.0					
Authorization Bypass Through User-Controlled Key	04-May-2023	4.5	MeterSphere is an open source continuous testing platform, covering functions such as test tracking, interface	N/A	A-MET-METE-170523/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			testing, UI testing, and performance testing. This IDOR vulnerability allows the administrator of a project to modify other projects under the workspace. An attacker can obtain some operating permissions. The issue has been fixed in version 2.9.0. **CVE ID : CVE-2023-30550**		
Affected Version(s): 1.20.20-lts-79d354a6					
N/A	08-May-2023	9.8	Metersphere v1.20.20-lts-79d354a6 is vulnerable to Remote Command Execution. The system command reverse-shell can be executed at the custom code snippet function of the metersphere system workbench **CVE ID : CVE-2023-29944**	N/A	A-MET-METE-170523/607
Vendor: microbin					
Product: microbin					
Affected Version(s): 1.2.0					
Improper Neutralization of Input During Web Page Generation	04-May-2023	5.4	A cross-site scripting vulnerability (XSS) in the component microbin/src/pasta.rs of Microbin v1.2.0 allows attackers to execute arbitrary	https://github.com/szabodanika/microbin/pull/143	A-MIC-MICR-170523/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			web scripts or HTML via a crafted payload. **CVE ID : CVE-2023-27075**		
Vendor: Microsoft					
Product: 365_apps					
Affected Version(s): -					
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	A-MIC-365_-170523/609
N/A	09-May-2023	3.3	Microsoft Access Denial of Service Vulnerability **CVE ID : CVE-2023-29333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29333	A-MIC-365_-170523/610
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 113.0.1774.35					
N/A	05-May-2023	7.5	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-29350**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29350	A-MIC-EDGE-170523/611
N/A	05-May-2023	4.7	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29354**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29354	A-MIC-EDGE-170523/612
Product: office					
Affected Version(s): 2019					
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulner	A-MIC-OFFI-170523/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29335	ability/CVE-2023-29335	
N/A	09-May-2023	3.3	Microsoft Access Denial of Service Vulnerability **CVE ID : CVE-2023-29333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29333	A-MIC-OFFI-170523/614
Affected Version(s): 2021					
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	A-MIC-OFFI-170523/615
N/A	09-May-2023	3.3	Microsoft Access Denial of Service Vulnerability **CVE ID : CVE-2023-29333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29333	A-MIC-OFFI-170523/616
Product: remote_desktop					
Affected Version(s): * Up to (excluding) 10.2.3006.0					
N/A	09-May-2023	5.3	Microsoft Remote Desktop app for Windows Information Disclosure Vulnerability **CVE ID : CVE-2023-28290**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28290	A-MIC-REMO-170523/617
Product: sharepoint_enterprise_server					
Affected Version(s): 2016					
N/A	09-May-2023	6.5	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-24950**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24950	A-MIC-SHAR-170523/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sharepoint_server					
Affected Version(s): -					
N/A	09-May-2023	6.5	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-24950**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24950	A-MIC-SHAR-170523/619
Affected Version(s): 2019					
N/A	09-May-2023	6.5	Microsoft SharePoint Server Spoofing Vulnerability **CVE ID : CVE-2023-24950**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24950	A-MIC-SHAR-170523/620
Product: word					
Affected Version(s): 2016					
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	A-MIC-WORD-170523/621
Affected Version(s): 2013					
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	A-MIC-WORD-170523/622
Vendor: monicahq					
Product: monica					
Affected Version(s): 4.0.0					
N/A	08-May-2023	8.8	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the	N/A	A-MON-MONI-170523/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application via CSTI in the `people:id/food` endpoint and food parameter. **CVE ID : CVE-2023-1094**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/introductions` endpoint and first_met_additional_info parameter. **CVE ID : CVE-2023-30787**	https://www.monicahq.com/	A-MON-MONI-170523/624
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people/add` endpoint and nickName, description, lastName, middleName and firstName parameter. **CVE ID : CVE-2023-30788**	https://www.monicahq.com/	A-MON-MONI-170523/625
Improper Neutralization of Input	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to	https://www.monicahq.com/	A-MON-MONI-170523/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			execute malicious code in the application via CSTI in the `people:id/work` endpoint and job and company parameter. **CVE ID : CVE-2023-30789**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	MonicaHQ version 4.0.0 allows an authenticated remote attacker to execute malicious code in the application via CSTI in the `people:id/relationships` endpoint and first_name and last_name parameter. **CVE ID : CVE-2023-30790**	https://www.monicahq.com/	A-MON-MONI-170523/627
Vendor: Moodle					
Product: moodle					
Affected Version(s): From (including) 3.11.0 Up to (excluding) 3.11.14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&	A-MOO-MOOD-170523/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			within the application database. **CVE ID : CVE-2023-30944**	st=commit&s=MDL-77187	
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.21					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. **CVE ID : CVE-2023-30944**	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77187	A-MOO-MOOD-170523/629
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database.	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&	A-MOO-MOOD-170523/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30944	s=MDL-77187	
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. **CVE ID : CVE-2023-30944**	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77187	A-MOO-MOOD-170523/631
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. **CVE ID : CVE-2023-30943**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77718, https://moodle.org/mod/forum/discuss.php?d=446285, https://bugzilla.redhat.com/show_bug.cgi?id=2188605	A-MOO-MOOD-170523/632
Vendor: multi_language_hotel_management_software_project					
Product: multi_language_hotel_management_software					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-May-2023	6.1	A vulnerability has been found in SourceCodester Multi Language Hotel Management Software 1.0 and classified as problematic. This vulnerability affects unknown code of the file ajax.php of the component POST Parameter Handler. The manipulation of the argument complaint_type with the input <script>alert(document.cookie)</script> 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-228172. **CVE ID : CVE-2023-2565**	N/A	A-MUL-MULT-170523/633
Vendor: mutagen					
Product: mutagen					
Affected Version(s): * Up to (excluding) 0.16.6					
Improper Encoding or Escaping of Output	08-May-2023	8.8	Mutagen provides real-time file synchronization and flexible network forwarding for developers. Prior to versions 0.16.6 and	https://github.com/mutagen-io/mutagen/security/advisories/GHS	A-MUT-MUTA-170523/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.17.1 in `mutagen` and prior to version 0.17.1 in `mutagen-compose`, Mutagen `list` and `monitor` commands are susceptible to control characters that could be provided by remote endpoints. This could cause terminal corruption, either intentional or unintentional, if these characters were present in error messages or file paths/names. This could be used as an attack vector if synchronizing with an untrusted remote endpoint, synchronizing files not under control of the user, or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be	A-jmp2-wc4p-wfh2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. **CVE ID : CVE-2023-30844**		
Affected Version(s): 0.17.0					
Improper Encoding or Escaping of Output	08-May-2023	8.8	Mutagen provides real-time file synchronization and flexible network forwarding for developers. Prior to versions 0.16.6 and 0.17.1 in `mutagen` and prior to version 0.17.1 in `mutagen-compose`, Mutagen `list` and `monitor` commands are susceptible to control characters that could be provided by remote endpoints. This could cause terminal corruption, either intentional or unintentional, if these characters were present in error messages or file paths/names. This could be used as an attack vector if	https://github.com/mutagen-io/mutagen/security/advisories/GHSA-jmp2-wc4p-wfh2	A-MUT-MUTA-170523/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			synchronizing with an untrusted remote endpoint, synchronizing files not under control of the user, or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. **CVE ID : CVE-2023-30844**		
Product: mutagen_compose					
Affected Version(s): * Up to (excluding) 0.17.1					
Improper Encoding or	08-May-2023	8.8	Mutagen provides real-time file synchronization and flexible network	https://github.com/mutagen-io/mutagen/	A-MUT-MUTA-170523/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			forwarding for developers. Prior to versions 0.16.6 and 0.17.1 in `mutagen` and prior to version 0.17.1 in `mutagen-compose`, Mutagen `list` and `monitor` commands are susceptible to control characters that could be provided by remote endpoints. This could cause terminal corruption, either intentional or unintentional, if these characters were present in error messages or file paths/names. This could be used as an attack vector if synchronizing with an untrusted remote endpoint, synchronizing files not under control of the user, or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of	security/advisories/GHSA-jmp2-wc4p-wfh2	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk. **CVE ID : CVE-2023-30844**		
Vendor: netentsec					
Product: application_security_gateway					
Affected Version(s): 6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-May-2023	9.8	NS-ASG v6.3 was discovered to contain a SQL injection vulnerability via the component /admin/add_ikev2.php. **CVE ID : CVE-2023-30242**	N/A	A-NET-APPL-170523/637
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-May-2023	7.5	Beijing Netcon NS-ASG Application Security Gateway v6.3 is vulnerable to SQL Injection via TunnelId that allows access to sensitive information. **CVE ID : CVE-2023-30243**	N/A	A-NET-APPL-170523/638
Vendor: newbee-mall_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: newbee-mall					
Affected Version(s): * Up to (excluding) 2022-10-27					
Authorization Bypass Through User-Controlled Key	04-May-2023	5.4	Insecure permissions in the updateUserInfo function of newbee-mall before commit 1f2c2dfy allows attackers to obtain user account information. **CVE ID : CVE-2023-30216**	N/A	A-NEW-NEWB-170523/639
Vendor: newbinggogo_project					
Product: newbinggogo					
Affected Version(s): * Up to (including) 2023.5.5.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	6.1	A vulnerability was found in jja8 NewBingGoGo up to 2023.5.5.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. 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-228167. **CVE ID : CVE-2023-2560**	N/A	A-NEW-NEWB-170523/640
Vendor: obsidian					
Product: obsidian					
Affected Version(s): 1.1.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	01-May-2023	7.5	An issue discovered in Obsidian Canvas 1.1.9 allows remote attackers to send desktop notifications, record user audio and other unspecified impacts via embedded website on the canvas page. **CVE ID : CVE-2023-27035**	N/A	A-OBS-OBSI-170523/641
Vendor: octopus					
Product: octopus_deploy					
Affected Version(s): From (including) 2018.3.0 Up to (excluding) 2022.3.10929					
N/A	02-May-2023	5.3	In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview function **CVE ID : CVE-2023-2247**	https://advisories.octopus.com/post/2023/sa2023-07/	A-OCT-OCTO-170523/642
Affected Version(s): From (including) 2022.4.0 Up to (excluding) 2022.4.8319					
N/A	02-May-2023	5.3	In affected versions of Octopus Deploy it is possible to unmask variable secrets using the variable preview function **CVE ID : CVE-2023-2247**	https://advisories.octopus.com/post/2023/sa2023-07/	A-OCT-OCTO-170523/643
Vendor: olevmedia					
Product: olevmedia_shortcodes					
Affected Version(s): * Up to (including) 1.1.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Olevmedia Olevmedia Shortcodes plugin <= 1.1.9 versions. **CVE ID : CVE-2023-25798**	N/A	A-OLE-OLEV-170523/644
Vendor: online_dj_management_system_project					
Product: online_dj_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-May-2023	9.8	A vulnerability was found in SourceCodester Online DJ Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/bookings/view_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-227795. **CVE ID : CVE-2023-2451**	N/A	A-ONL-ONLI-170523/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: online_food_ordering_system_project					
Product: online_food_ordering_system					
Affected Version(s): 2.0					
Unrestricted Upload of File with Dangerous Type	05-May-2023	9.8	An arbitrary file upload vulnerability in the component /admin/ajax.php?action=save_menu of Online Food Ordering System v2.0 allows attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID : CVE-2023-30122**	N/A	A-ONL-ONLI-170523/646
Vendor: online_pizza_ordering_system_project					
Product: online_pizza_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-May-2023	9.8	SourceCodester Online Pizza Ordering System v1.0 is vulnerable to SQL Injection via the QTY parameter. **CVE ID : CVE-2023-30092**	N/A	A-ONL-ONLI-170523/647
Vendor: online_reviewer_system_project					
Product: online_reviewer_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	09-May-2023	9.8	A vulnerability was found in SourceCodester Online Reviewer System 1.0 and classified as critical. Affected by this issue is some unknown	N/A	A-ONL-ONLI-170523/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			functionality of the file /reviewer/system/system/admins/manage/users/user-update.php of the component GET Parameter Handler. The manipulation of the argument user_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228398 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2596**		
Vendor: online_tours_\&_travels_management_system_project					
Product: online_tours_\&_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-May-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Tours & Travels Management System 1.0. This affects the function exec of the file disapprove_delete.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	N/A	A-ONL-ONLI-170523/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The identifier VDB-228549 was assigned to this vulnerability. **CVE ID : CVE-2023-2619**		
Vendor: onosproject					
Product: onos					
Affected Version(s): From (including) 1.9.0 Up to (including) 2.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-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 or HTML via a crafted payload injected into the url parameter of the API documentation dashboard. **CVE ID : CVE-2023-30093**	N/A	A-ONO-ONOS-170523/650
Vendor: Open-emr					
Product: openemr					
Affected Version(s): * Up to (excluding) 7.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2566**	https://github.com/openemr/openemr/commit/a2adac7320dfc631b1da688c3b04f54b8240fc7b, https://huntr.dev/bounties/47d6fc2a	A-OPE-OPEN-170523/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-989a-44eb-9cb7-ab4f8bd44496	
Vendor: openproject					
Product: openproject					
Affected Version(s): From (including) 7.4.0 Up to (excluding) 12.5.4					
Insufficient Session Expiration	08-May-2023	6.5	OpenProject is open source project management software. Starting with version 7.4.0 and prior to version 12.5.4, when a user registers and confirms their first two-factor authentication (2FA) device for an account, existing logged in sessions for that user account are not terminated. Likewise, if an administrators creates a mobile phone 2FA device on behalf of a user, their existing sessions are not terminated. The issue has been resolved in OpenProject version 12.5.4 by actively terminating sessions of user accounts having registered and confirmed a 2FA device. As a workaround, users who register the first 2FA device on their account can	https://github.com/opf/openproject/security/advisories/GHSA-xfp9-qqfj-x28q, https://github.com/opf/openproject/pull/12508	A-OPE-OPEN-170523/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manually log out to terminate all other active sessions. This is the default behavior of OpenProject but might be disabled through a configuration option. Double check that this option is not overridden if one plans to employ the workaround. **CVE ID : CVE-2023-31140**		
Vendor: opentsdb					
Product: opentsdb					
Affected Version(s): From (including) 1.0.0 Up to (including) 2.4.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-May-2023	9.8	Due to insufficient validation of parameters passed to the legacy HTTP query API, it is possible to inject crafted OS commands into multiple parameters and execute malicious code on the OpenTSDB host system. This exploit exists due to an incomplete fix that was made when this vulnerability was previously disclosed as CVE-2020-35476. Regex validation that was implemented to restrict allowed	https://github.com/OpenTSDB/opentsdb/pull/2275	A-OPE-OPEN-170523/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			input to the query API does not work as intended, allowing crafted commands to bypass validation. **CVE ID : CVE-2023-25826**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Due to insufficient validation of parameters reflected in error messages by the legacy HTTP query API and the logging endpoint, it is possible to inject and execute malicious JavaScript within the browser of a targeted OpenTSDB user. This issue shares the same root cause as CVE-2018-13003, a reflected XSS vulnerability with the suggestion endpoint. **CVE ID : CVE-2023-25827**	https://github.com/OpenTSDB/opentsdb/pull/2274	A-OPE-OPEN-170523/654
Vendor: oxilab					
Product: accordions					
Affected Version(s): * Up to (excluding) 2.3.1					
Improper Neutralization of	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-OXI-ACCO-170523/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in Biplob Adhikari Accordion – Multiple Accordion or FAQs Builder plugin <= 2.3.0 versions. **CVE ID : CVE-2023-25962**		
Vendor: palletsprojects					
Product: flask					
Affected Version(s): * Up to (excluding) 2.2.5					
Use of Persistent Cookies Containing Sensitive Information	02-May-2023	7.5	Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response containing data intended for one client may be cached and subsequently sent by the proxy to other clients. If the proxy also caches `Set-Cookie` headers, it may send one client's `session` cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior regarding cookies. The risk depends on all these conditions being met. 1. The application must be hosted behind a caching proxy that does not	https://github.com/pallets/flask/commit/70f906c51ce49c485f1d355703e9cc3386b1cc2b, https://github.com/pallets/flask/security/advisories/GHSA-m2qf-hxjv-5gpq, https://github.com/pallets/flask/commit/afd63b16170b7c047f5758eb910c416511e9c965	A-PAL-FLAS-170523/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			strip cookies or ignore responses with cookies. 2. The application sets `session.permanent = True` 3. The application does not access or modify the session at any point during a request. 4. `SESSION_REFRESH_EACH_REQUEST` enabled (the default). 5. The application does not set a `Cache-Control` header to indicate that a page is private or should not be cached. This happens because vulnerable versions of Flask only set the `Vary: Cookie` header when the session is accessed or modified, not when it is refreshed (re-sent to update the expiration) without being accessed or modified. This issue has been fixed in versions 2.3.2 and 2.2.5.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30861		
Affected Version(s): From (including) 2.3.0 Up to (excluding) 2.3.2					
Use of Persistent Cookies Containing Sensitive Information	02-May-2023	7.5	Flask is a lightweight WSGI web application framework. When all of the following conditions are met, a response containing data intended for one client may be cached and subsequently sent by the proxy to other clients. If the proxy also caches `Set-Cookie` headers, it may send one client's `session` cookie to other clients. The severity depends on the application's use of the session and the proxy's behavior regarding cookies. The risk depends on all these conditions being met. 1. The application must be hosted behind a caching proxy that does not strip cookies or ignore responses with cookies. 2. The application sets `session.permanent = True`	https://github.com/pallets/flask/commit/70f906c51ce49c485f1d355703e9cc3386b1cc2b, https://github.com/pallets/flask/security/advisories/GHSA-m2qf-hxjv-5gpq, https://github.com/pallets/flask/commit/afd63b16170b7c047f5758eb910c416511e9c965	A-PAL-FLAS-170523/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3. The application does not access or modify the session at any point during a request. 4. `SESSION_REFRESH_EACH_REQUEST` enabled (the default). 5. The application does not set a `Cache-Control` header to indicate that a page is private or should not be cached. This happens because vulnerable versions of Flask only set the `Vary: Cookie` header when the session is accessed or modified, not when it is refreshed (re-sent to update the expiration) without being accessed or modified. This issue has been fixed in versions 2.3.2 and 2.2.5. **CVE ID : CVE-2023-30861**		
Vendor: peepso					
Product: peepso					
Affected Version(s): * Up to (excluding) 6.0.3.0					
Cross-Site Request	03-May-2023	8.8	Cross-Site Request Forgery (CSRF)	N/A	A-PEE-PEEP-170523/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerability in PeepSo Community by PeepSo plugin <= 6.0.2.0 versions. **CVE ID : CVE-2023-25967**		
Vendor: perfreeblog_project					
Product: perfreeblog					
Affected Version(s): 3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	5.4	Cross Site Scripting (XSS) vulnerability in PerfreeBlog 3.1.2 allows attackers to execute arbitrary code via the Post function. **CVE ID : CVE-2023-29643**	https://github.com/perfree/PerfreeBlog/issues/14	A-PER-PERF-170523/659
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-May-2023	4.8	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.13. **CVE ID : CVE-2023-2427**	https://github.com/thorsten/phpmyfaq/commit/514f4df2ad918e69575028d58b2e33aaf536e59b, https://huntr.dev/bounties/89005a6d-d019-4cb7-ae88-486d2d44190d	A-PHP-PHPM-170523/660
Improper Neutralization of Input	05-May-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository	https://github.com/thorsten/phpmyfaq/commit/2	A-PHP-PHPM-170523/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			thorsten/phpmyfaq prior to 3.1.13. **CVE ID : CVE-2023-2550**	0ac51594db11604a4518aacc28a51f67d4f11bf, https://huntr.dev/bounties/840c8d91-c97e-4116-a9f8-4ab1a38d239b	
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.5.18					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-May-2023	7.5	Pimcore is an open source data and experience management platform. Versions of Pimcore prior to 10.5.18 are vulnerable to path traversal. The impact of this path traversal and arbitrary extension is limited to creation of arbitrary files and appending data to existing files. When combined with the SQL Injection, the exported data `RESTRICTED DIFFUSION 9 / 9` can be controlled and a webshell can be uploaded. Attackers can use that to execute arbitrary PHP code on the server with the permissions of the	https://github.com/pimcore/pimcore/security/advisories/GHSA-g2mc-fqqc-hxg3, https://github.com/pimcore/pimcore/commit/f1d904094700b513c4756904fa2b1e19d08d890e.patch, https://github.com/pimcore/pimcore/pull/14498	A-PIM-PIMC-170523/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver. Users may upgrade to version 10.5.18 to receive a patch or, as a workaround, apply the patch manually. **CVE ID : CVE-2023-30855**		
Affected Version(s): * Up to (excluding) 10.5.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	5.4	Cross-site Scripting (XSS) - Generic in GitHub repository pimcore/pimcore prior to 10.5.21. **CVE ID : CVE-2023-2616**	https://github.com/pimcore/pimcore/commit/07a2c95be524c7e20105cef58c5767d4ebb06091, https://huntr.dev/bounties/564cb512-2bcc-4458-8c20-88110ab45801	A-PIM-PIMC-170523/663
Vendor: pixelyoursite					
Product: product_catalog_feed					
Affected Version(s): * Up to (excluding) 2.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	The Product Catalog Feed by PixelYourSite WordPress plugin before 2.1.1 does not sanitise and escape the edit parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high	N/A	A-PIX-PROD-170523/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege users such as administrators. **CVE ID : CVE-2023-1804**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	The Product Catalog Feed by PixelYourSite WordPress plugin before 2.1.1 does not sanitise and escape the page parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-1805**	N/A	A-PIX-PROD-170523/665
Vendor: plainviewplugins					
Product: mycryptocheckout					
Affected Version(s): * Up to (excluding) 2.124					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	6.1	The MyCryptoCheckout WordPress plugin before 2.124 does not escape some URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2023-1546**	N/A	A-PLA-MYCR-170523/666
Vendor: plugin-planet					
Product: dashboard_widget_suite					
Affected Version(s): * Up to (excluding) 3.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jeff Starr Dashboard Widgets Suite plugin <= 3.2.1 versions. **CVE ID : CVE-2023-26517**	N/A	A-PLU-DASH-170523/667
Vendor: podofo_project					
Product: podofo					
Affected Version(s): 0.10.0					
Use After Free	10-May-2023	8.8	Podofo v0.10.0 was discovered to contain a heap-use-after-free via the component PoDoFo::PdfEncrypt::IsMetadataEncrypted(). **CVE ID : CVE-2023-31566**	https://github.com/podofo/podofo/issues/70	A-POD-PODO-170523/668
Out-of-bounds Write	10-May-2023	8.8	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncryptAESV3::PdfEncryptAESV3. **CVE ID : CVE-2023-31567**	https://github.com/podofo/podofo/issues/71	A-POD-PODO-170523/669
Out-of-bounds Write	10-May-2023	8.8	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncryptRC4::PdfEncryptRC4.	https://github.com/podofo/podofo/issues/72	A-POD-PODO-170523/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31568		
Vendor: Podsfoundation					
Product: pods					
Affected Version(s): * Up to (excluding) 2.9.11					
Cross-Site Request Forgery (CSRF)	03-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Pods Framework Team Pods – Custom Content Types and Fields plugin <= 2.9.10.2 versions. **CVE ID : CVE-2023-23790**	N/A	A-POD-PODS-170523/671
Vendor: premmerce					
Product: premmerce_redirect_manager					
Affected Version(s): * Up to (including) 1.0.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Premmerce Premmerce Redirect Manager plugin <= 1.0.9 versions. **CVE ID : CVE-2023-23789**	N/A	A-PRE-PREM-170523/672
Vendor: Prestashop					
Product: prestashop					
Affected Version(s): 1.7.7.4					
Improper Neutralization of Input During Web Page Generation	11-May-2023	6.1	A cross-site scripting (XSS) vulnerability in PrestaShop v1.7.7.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the	N/A	A-PRE-PRES-170523/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			message parameter in /contactform/contactform.php. **CVE ID : CVE-2023-31508**		
Product: scexportcustomers					
Affected Version(s): * Up to (including) 3.6.1					
N/A	04-May-2023	7.5	PrestaShop scexportcustomers <= 3.6.1 is vulnerable to Incorrect Access Control. Due to a lack of permissions' control, a guest can access exports from the module which can lead to leak of personal information from customer table. **CVE ID : CVE-2023-30282**	N/A	A-PRE-SCEX-170523/674
Vendor: profilepress					
Product: profilepress					
Affected Version(s): * Up to (excluding) 4.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.4 versions. **CVE ID : CVE-2023-23830**	N/A	A-PRO-PROF-170523/675
Vendor: properfraction					
Product: profilepress					
Affected Version(s): * Up to (excluding) 4.5.5					
Improper Neutralizat	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site	N/A	A-PRO-PROF-170523/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.4 versions. **CVE ID : CVE-2023-23820**		
Vendor: publish_to_schedule_project					
Product: publish_to_schedule					
Affected Version(s): * Up to (excluding) 4.5.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alex Benfica Publish to Schedule plugin <= 4.5.4 versions. **CVE ID : CVE-2023-26519**	N/A	A-PUB-PUBL-170523/677
Vendor: Puppet					
Product: puppet_enterprise					
Affected Version(s): 2021.7.1					
N/A	04-May-2023	5.3	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations. **CVE ID : CVE-2023-1894**	https://www.puppet.com/security/cve/cve-2023-1894-puppet-server-redos	A-PUP-PUPP-170523/678
Affected Version(s): 2023.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-May-2023	5.3	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations. **CVE ID : CVE-2023-1894**	https://www.puppet.com/security/cve/cve-2023-1894-puppet-server-redos	A-PUP-PUPP-170523/679
Product: puppet_server					
Affected Version(s): 7.9.2					
N/A	04-May-2023	5.3	A Regular Expression Denial of Service (ReDoS) issue was discovered in Puppet Server 7.9.2 certificate validation. An issue related to specifically crafted certificate names significantly slowed down server operations. **CVE ID : CVE-2023-1894**	https://www.puppet.com/security/cve/cve-2023-1894-puppet-server-redos	A-PUP-PUPP-170523/680
Vendor: qbian61_forum-java_project					
Product: qbian61_forum-java					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	01-May-2023	6.1	Cross Site Scripting (XSS) vulnerability in Qbian61 forum-java, allows attackers to inject arbitrary web script or HTML via editing the article	N/A	A-QBI-QBIA-170523/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			content in the "article editor" page. **CVE ID : CVE-2023-29637**		
Vendor: quantumcloud					
Product: ai_chatbot					
Affected Version(s): * Up to (excluding) 4.4.5					
Cross-Site Request Forgery (CSRF)	08-May-2023	6.1	The AI ChatBot WordPress plugin before 4.4.5 does not escape most of its settings before outputting them back in the dashboard, and does not have a proper CSRF check, allowing attackers to make a logged in admin set XSS payloads in them. **CVE ID : CVE-2023-1011**	N/A	A-QUA-AI_C-170523/682
Affected Version(s): * Up to (excluding) 4.4.7					
Deserialization of Untrusted Data	08-May-2023	9.8	The AI ChatBot WordPress plugin before 4.4.7 unserializes user input from cookies via an AJAX action available to unauthenticated users, which could allow them to perform PHP Object Injection when a suitable gadget is present on the blog **CVE ID : CVE-2023-1650**	N/A	A-QUA-AI_C-170523/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.4.9					
Cross-Site Request Forgery (CSRF)	08-May-2023	6.1	The AI ChatBot WordPress plugin before 4.4.9 does not have authorisation and CSRF in a function hooked to init, allowing unauthenticated users to update some settings, leading to Stored XSS due to the lack of escaping when outputting them in the admin dashboard **CVE ID : CVE-2023-1660**	N/A	A-QUA-AI_C-170523/684
Cross-Site Request Forgery (CSRF)	08-May-2023	5.4	The AI ChatBot WordPress plugin before 4.4.9 does not have authorisation and CSRF in the AJAX action responsible to update the OpenAI settings, allowing any authenticated users, such as subscriber to update them. Furthermore, due to the lack of escaping of the settings, this could also lead to Stored XSS **CVE ID : CVE-2023-1651**	N/A	A-QUA-AI_C-170523/685
Affected Version(s): * Up to (excluding) 4.5.1					
Improper Neutralization of Input	08-May-2023	4.8	The AI ChatBot WordPress plugin before 4.5.1 does not sanitise and escape	N/A	A-QUA-AI_C-170523/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			numerous of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-1649**		
Vendor: rediker					
Product: adminplus					
Affected Version(s): 6.1.91.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	Cross Site Scripting (XSS) vulnerability in Rediker Software AdminPlus 6.1.91.00 allows remote attackers to run arbitrary code via the onload function within the application DOM. **CVE ID : CVE-2023-24744**	N/A	A-RED-ADMI-170523/687
Vendor: return_and_warranty_management_system_for_woocommerce_project					
Product: return_and_warranty_management_system_for_woocommerce					
Affected Version(s): * Up to (including) 1.2.3					
Improper Neutralization of Input During Web Page Generation	08-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in chilidevs Return and Warranty Management System for WooCommerce	N/A	A-RET-RETU-170523/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 1.2.3 versions. **CVE ID : CVE-2023-22710**		
Vendor: rosariosis					
Product: rosariosis					
Affected Version(s): 10.8.4					
Improper Neutralization of Formula Elements in a CSV File	02-May-2023	5.4	RosarioSIS 10.8.4 is vulnerable to CSV injection via the Periods Module. **CVE ID : CVE-2023-29918**	N/A	A-ROS-ROSA-170523/689
Vendor: S-cms					
Product: S-cms					
Affected Version(s): 5.0					
N/A	05-May-2023	7.2	S-CMS v5.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the component /admin/ajax.php. **CVE ID : CVE-2023-29963**	N/A	A-S-C-S-CM-170523/690
Vendor: Samsung					
Product: samsung_blockchain_keystore					
Affected Version(s): * Up to (excluding) 1.3.12.1					
Out-of-bounds Write	04-May-2023	7.8	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA_ARRAY command in bc_tui trustlet from Samsung Blockchain	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=05	A-SAM-SAMS-170523/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-21506**		
Out-of-bounds Write	04-May-2023	7.8	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-21508**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=05	A-SAM-SAMS-170523/692
Out-of-bounds Write	04-May-2023	7.8	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_UPDATE_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code. **CVE ID : CVE-2023-21509**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=05	A-SAM-SAMS-170523/693
Out-of-bounds Read	04-May-2023	5.5	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA_ARRAY command in	https://security.samsungmobile.com/serviceWeb.smsb?year=2	A-SAM-SAMS-170523/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory. **CVE ID : CVE-2023-21507**	023&month=05	
Out-of-bounds Read	04-May-2023	5.5	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_UPDATE_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory. **CVE ID : CVE-2023-21510**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=05	A-SAM-SAMS-170523/695
Out-of-bounds Read	04-May-2023	5.5	Out-of-bounds Read vulnerability while processing CMD_COLDWALLET_BTC_SET_PRV_UTXO in bc_core trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory. **CVE ID : CVE-2023-21511**	https://security.samsungmobile.com/serviceWeb.smsb?year=2023&month=05	A-SAM-SAMS-170523/696
Product: samsung_core_services					
Affected Version(s): * Up to (excluding) 2.1.00.36					
N/A	04-May-2023	8.6	Improper access control in Samsung	https://security.samsung	A-SAM-SAMS-170523/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Core Service prior to version 2.1.00.36 allows attacker to write arbitrary file in sandbox. **CVE ID : CVE-2023-21505**	mobile.com/serviceWeb.smsb?year=2023&month=05	
Vendor: sandhillsdev					
Product: easy_digital_downloads					
Affected Version(s): From (including) 3.1 Up to (excluding) 3.1.1.4.2					
Improper Authentication	02-May-2023	9.8	Improper Authentication vulnerability in Easy Digital Downloads plugin allows unauth. Privilege Escalation. This issue affects Easy Digital Downloads: from 3.1 through 3.1.1.4.1. **CVE ID : CVE-2023-30869**	https://patchstack.com/articles/critical-easy-digital-downloads-vulnerability?_s_id=cve	A-SAN-EASY-170523/698
Vendor: SAP					
Product: businessobjects					
Affected Version(s): 4.20					
Insufficiently Protected Credentials	09-May-2023	5.9	SAP BusinessObjects Platform - versions 420, 430, Information design tool transmits sensitive information as cleartext in the binaries over the network. This could allow an unauthenticated attacker with deep knowledge to gain sensitive information such as user credentials and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			domain names, which may have a low impact on confidentiality and no impact on the integrity and availability of the system. **CVE ID : CVE-2023-28764**		
Affected Version(s): 4.30					
Insufficiently Protected Credentials	09-May-2023	5.9	SAP BusinessObjects Platform - versions 420, 430, Information design tool transmits sensitive information as cleartext in the binaries over the network. This could allow an unauthenticated attacker with deep knowledge to gain sensitive information such as user credentials and domain names, which may have a low impact on confidentiality and no impact on the integrity and availability of the system. **CVE ID : CVE-2023-28764**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: businessobjects_business_intelligence					
Affected Version(s): 420					
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	7.6	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality, limited impact on integrity and availability of the application. **CVE ID : CVE-2023-30740**	https://launchpad.support.sap.com/#/notes/3313484, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/701
N/A	09-May-2023	7.2	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker with administrator privileges to get the login token of any logged-in BI user over the network without any user interaction. The attacker can impersonate any user on the platform resulting into accessing and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying data. The attacker can also make the system partially or entirely unavailable. **CVE ID : CVE-2023-28762**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-30741**	https://launchpad.support.sap.com/#/notes/3309935, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/703
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted	https://launchpad.support.sap.com/#/notes/3319400, https://www.sap.com/documents/2022/02/fa86	A-SAP-BUSI-170523/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-31406**	5ea4-167e-0010-bca6-c68f7e60039b.html	
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	5	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (Central Management Service) - versions 420, 430, allows an attacker to access information which would otherwise be restricted. Some users with specific privileges could have access to credentials of other users. It could let them access data sources which would otherwise be restricted. **CVE ID : CVE-2023-31404**	https://launchpad.support.sap.com/#/notes/3038911, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/705
Affected Version(s): 430					
Exposure of Sensitive	09-May-2023	7.6	SAP BusinessObjects Business Intelligence	https://launchpad.suppo	A-SAP-BUSI-170523/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			Platform - versions 420, 430, allows an authenticated attacker to access sensitive information which is otherwise restricted. On successful exploitation, there could be a high impact on confidentiality, limited impact on integrity and availability of the application. **CVE ID : CVE-2023-30740**	rt.sap.com/#/notes/3313484, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
N/A	09-May-2023	7.2	SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an authenticated attacker with administrator privileges to get the login token of any logged-in BI user over the network without any user interaction. The attacker can impersonate any user on the platform resulting into accessing and modifying data. The attacker can also make the system	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			partially or entirely unavailable. **CVE ID : CVE-2023-28762**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-30741**	https://launchpad.support.sap.com/#/notes/3309935, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/708
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to insufficient input validation, SAP BusinessObjects Business Intelligence Platform - versions 420, 430, allows an unauthenticated attacker to redirect users to untrusted site using a malicious link. On successful exploitation, an	https://launchpad.support.sap.com/#/notes/3319400, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-BUSI-170523/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can view or modify information causing a limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-31406**	c68f7e60039b.html	
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	5	Under certain conditions, SAP BusinessObjects Business Intelligence Platform (Central Management Service) - versions 420, 430, allows an attacker to access information which would otherwise be restricted. Some users with specific privileges could have access to credentials of other users. It could let them access data sources which would otherwise be restricted. **CVE ID : CVE-2023-31404**	https://launchpad.support.sap.com/#/notes/3038911, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/710
Product: business_planning_and_consolidation					
Affected Version(s): 740					
Improper Neutralization of Input	09-May-2023	5.4	SAP Business Planning and Consolidation - versions 740, 750,	https://launchpad.support.sap.com/#/notes/3312	A-SAP-BUSI-170523/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			allows an authorized attacker to upload a malicious file, resulting in Cross-Site Scripting vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-31407**	892, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 750					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP Business Planning and Consolidation - versions 740, 750, allows an authorized attacker to upload a malicious file, resulting in Cross-Site Scripting vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2023-31407**	https://launchpad.support.sap.com/#/notes/3312892, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170523/712
Product: customer_relationship_management_s4fnd					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 102					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/713
Affected Version(s): 103					
Improper Neutralizat	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND	https://launchpad.suppo	A-SAP-CUST-170523/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	rt.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 104					
Improper Neutralization of Input During	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106,	https://launchpad.support.sap.com/#/notes/3315971,	A-SAP-CUST-170523/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 105					
Improper Neutralization of Input During Web Page Generation	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701,	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2	A-SAP-CUST-170523/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 106					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747,	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-CUST-170523/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	c68f7e60039b.html	
Affected Version(s): 107					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Product: customer_relationship_management_webclient_ui					
Affected Version(s): 7.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Affected Version(s): 7.31					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Affected Version(s): 7.46					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/721
Affected Version(s): 7.47					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/722
Affected Version(s): 7.48					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Affected Version(s): 700					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Affected Version(s): 701					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Affected Version(s): 731					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Affected Version(s): 746					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Affected Version(s): 747					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Affected Version(s): 748					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modified or read by the attacker. **CVE ID : CVE-2023-30742**		
Affected Version(s): 8.00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/730
Affected Version(s): 8.01					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-170523/731
Affected Version(s): 800					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731,	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa86	A-SAP-CUST-170523/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	5ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 801					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	SAP CRM (WebClient UI) - versions S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748,	https://launchpad.support.sap.com/#/notes/3315971, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-CUST-170523/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in a stored Cross-Site Scripting (XSS) vulnerability.An attacker could store a malicious URL and lure the victim to click, causing the script supplied by the attacker to execute in the victim user's session. The information from the victim's session could then be modified or read by the attacker. **CVE ID : CVE-2023-30742**	c68f7e60039b.html	
Product: gui_for_windows					
Affected Version(s): 8.0					
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	9.3	SAP GUI for Windows - version 7.70, 8.0, allows an unauthorized attacker to gain NTLM authentication information of a victim by tricking it into clicking a prepared shortcut file. Depending on the authorizations of the victim, the attacker can read	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3320467	A-SAP-GUI_-170523/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and modify potentially sensitive information after successful exploitation. **CVE ID : CVE-2023-32113**		
Affected Version(s): 7.70					
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	9.3	SAP GUI for Windows - version 7.70, 8.0, allows an unauthorized attacker to gain NTLM authentication information of a victim by tricking it into clicking a prepared shortcut file. Depending on the authorizations of the victim, the attacker can read and modify potentially sensitive information after successful exploitation. **CVE ID : CVE-2023-32113**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3320467	A-SAP-GUI_-170523/735
Product: netweaver_application_server_for_java					
Affected Version(s): 7.50					
Missing Authentication for Critical Function	09-May-2023	9.1	In SAP AS NetWeaver JAVA - versions SERVERCORE 7.50, J2EE-FRMW 7.50,	https://www.sap.com/documents/2022/02/fa865ea4-167e-	A-SAP-NETW-170523/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CORE-TOOLS 7.50, an unauthenticated attacker can attach to an open interface and make use of an open naming and directory API to instantiate an object which has methods which can be called without further authorization and authentication. A subsequent call to one of these methods can read or change the state of existing services without any effect on availability. **CVE ID : CVE-2023-30744**	0010-bca6-c68f7e60039b.html	
Product: powerdesigner_proxy					
Affected Version(s): 16.7					
Out-of-bounds Write	09-May-2023	7.5	In SAP PowerDesigner (Proxy) - version 16.7, an attacker can send a crafted request from a remote host to the proxy machine and crash the proxy server, due to faulty implementation of memory management causing a memory corruption. This leads to a high impact on	https://launchpad.support.sap.com/#/notes/3300624, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-POWE-170523/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability of the application. **CVE ID : CVE-2023-32111**		
Product: s4core					
Affected Version(s): 100					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4CO-170523/738
Product: s4fnd					
Affected Version(s): 102					
Improper Neutralizat	09-May-2023	5.4	SAP CRM WebClient UI - versions	https://www.sap.com/d	A-SAP-S4FN-170523/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	ocuments/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 103					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4FN-170523/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Affected Version(s): 104					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4FN-170523/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Affected Version(s): 105					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4FN-170523/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29188		
Affected Version(s): 106					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4FN-170523/743
Affected Version(s): 107					
Improper Neutralization of Input	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND	https://www.sap.com/documents/2022/02/fa86	A-SAP-S4FN-170523/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**	5ea4-167e-0010-bca6-c68f7e60039b.html	
Affected Version(s): 1.02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4FN-170523/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Product: sapscore					
Affected Version(s): 129					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	SAP CRM WebClient UI - versions SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SAPS-170523/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation, an attacker with user level access can read and modify some sensitive information but cannot delete the data. **CVE ID : CVE-2023-29188**		
Product: sapui5					
Affected Version(s): 750					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack. **CVE ID : CVE-2023-30743**	https://launchpad.support.sap.com/#/notes/3326210, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SAPU-170523/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 700					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack. **CVE ID : CVE-2023-30743**	https://launchpad.support.sap.com/#/notes/3326210, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SAPU-170523/748
Affected Version(s): 754					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This	https://launchpad.support.sap.com/#/notes/3326210, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-SAPU-170523/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack. **CVE ID : CVE-2023-30743**	c68f7e60039b.html	
Affected Version(s): 755					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack.	https://launchpad.support.sap.com/#/notes/3326210, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SAPU-170523/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30743		
Affected Version(s): 756					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack. **CVE ID : CVE-2023-30743**	https://launchpad.support.sap.com/#/notes/3326210, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-SAPU-170523/751
Affected Version(s): 757					
Improper Neutralization of Input During Web Page Generation	09-May-2023	6.1	Due to improper neutralization of input in SAPUI5 - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200,	https://launchpad.support.sap.com/#/notes/3326210, https://www.sap.com/documents/2	A-SAP-SAPU-170523/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			sap.m.FormattedText SAPUI5 control allows injection of untrusted CSS. This blocks user's interaction with the application. Further, in the absence of URL validation by the application, the vulnerability could lead to the attacker reading or modifying user's information through phishing attack. **CVE ID : CVE-2023-30743**	022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	
Product: vendor_master_hierarchy					
Affected Version(s): sap_appl_500					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**		
Affected Version(s): sap_appl_600					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/754
Affected Version(s): sap_appl_602					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/755
Affected Version(s): sap_appl_603					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**		
Affected Version(s): sap_appl_604					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32112		
Affected Version(s): sap_appl_605					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/758
Affected Version(s): sap_appl_606					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605,	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**		
Affected Version(s): sap_appl_616					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacting the integrity of the system. **CVE ID : CVE-2023-32112**		
Affected Version(s): sap_appl_617					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-VEND-170523/761
Affected Version(s): sap_appl_618					
Missing Authorization	09-May-2023	5.5	Vendor Master Hierarchy - versions SAP_APPL 500, SAP_APPL 600,	https://www.sap.com/documents/2022/02/fa86	A-SAP-VEND-170523/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100, does not perform necessary authorization checks for an authenticated user to access some of its function. This could lead to modification of data impacting the integrity of the system. **CVE ID : CVE-2023-32112**	5ea4-167e-0010-bca6-c68f7e60039b.html	
Vendor: scanservjs_project					
Product: scanservjs					
Affected Version(s): * Up to (excluding) 2.27.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-May-2023	10	OS Command Injection in GitHub repository sbs20/scanservjs prior to v2.27.0. **CVE ID : CVE-2023-2564**	https://github.com/sbs20/scanservjs/commit/d51fd52c1569813990b8f74e64ae6979c665dca1, https://huntr.dev/bounties/d13113ad-a107-416b-acc1-	A-SCA-SCAN-170523/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				01e4c16ec461	
Vendor: Sem-cms					
Product: Semcms					
Affected Version(s): 4.2					
Unrestricted Upload of File with Dangerous Type	05-May-2023	9.8	Semcms Shop v4.2 was discovered to contain an arbitrary file uplaod vulnerability via the component SEMCMS_Upfile.php. This vulnerability allows attackers to execute arbitrary code via uploading a crafted PHP file. **CVE ID : CVE-2023-30090**	N/A	A-SEM-SEMC-170523/764
Vendor: seopress					
Product: seopress					
Affected Version(s): * Up to (excluding) 6.5.0.3					
Deserialization of Untrusted Data	02-May-2023	7.2	The SEOPress WordPress plugin before 6.5.0.3 unserializes user input provided via the settings, which could allow high-privilege users such as admin to perform PHP Object Injection when a suitable gadget is present. **CVE ID : CVE-2023-1669**	N/A	A-SEO-SEOP-170523/765
Vendor: simple_portfolio_gallery_project					
Product: simple_portfolio_gallery					
Affected Version(s): 0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tauhidul Alam Simple Portfolio Gallery plugin <= 0.1 versions. **CVE ID : CVE-2023-26016**	N/A	A-SIM-SIMP-170523/766
Vendor: simple_youtube_responsive_project					
Product: simple_youtube_responsive					
Affected Version(s): * Up to (excluding) 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Eirudo Simple YouTube Responsive plugin <= 2.5 versions. **CVE ID : CVE-2023-25982**	N/A	A-SIM-SIMP-170523/767
Vendor: sloth_logo_customizer_project					
Product: sloth_logo_customizer					
Affected Version(s): * Up to (including) 2.0.2					
Cross-Site Request Forgery (CSRF)	08-May-2023	8.8	The Sloth Logo Customizer WordPress plugin through 2.0.2 does not have CSRF check when updating its settings, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	N/A	A-SLO-SLOT-170523/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0603		
Vendor: smtp_mailing_queue_project					
Product: smtp_mailing_queue					
Affected Version(s): * Up to (excluding) 2.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	The SMTP Mailing Queue WordPress plugin before 2.0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-1090**	N/A	A-SMT-SMTP-170523/769
Vendor: socket					
Product: engine.io					
Affected Version(s): From (including) 5.1.0 Up to (excluding) 6.4.2					
N/A	08-May-2023	6.5	Engine.IO is the implementation of transport-based cross-browser/cross-device bi-directional communication layer for Socket.IO. An uncaught exception vulnerability was introduced in version 5.1.0 and included in version 4.1.0 of the `socket.io` parent	https://github.com/socketio/engine.io/commit/fc480b4f305e16fe5972cf337d055e598372dc44, https://github.com/socketio/engine.io/security/advisories/GHSA-q9mw-68c2-j6m5	A-SOC-ENGI-170523/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package. Older versions are not impacted. A specially crafted HTTP request can trigger an uncaught exception on the Engine.IO server, thus killing the Node.js process. This impacts all the users of the `engine.io` package, including those who use depending packages like `socket.io`. This issue was fixed in version 6.4.2 of Engine.IO. There is no known workaround except upgrading to a safe version. **CVE ID : CVE-2023-31125**		
Vendor: sponsors_carousel_project					
Product: sponsors_carousel					
Affected Version(s): * Up to (including) 4.02					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sergey Panasenko Sponsors Carousel plugin <= 4.02 versions. **CVE ID : CVE-2023-23808**	N/A	A-SPO-SPON-170523/771
Vendor: sticky_ad_bar_project					
Product: sticky_ad_bar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bon Plan Gratos Sticky Ad Bar plugin <= 1.3.1 versions. **CVE ID : CVE-2023-25784**	N/A	A-STI-STIC-170523/772
Vendor: strikingly					
Product: strikingly					
Affected Version(s): *					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	08-May-2023	6.1	A prototype pollution vulnerability exists in Strikingly CMS which can result in reflected cross-site scripting (XSS) in affected applications and sites built with Strikingly. The vulnerability exists because of Strikingly JavaScript library parsing the URL fragment allows access to the __proto__ or constructor properties and the Object prototype. By leveraging an embedded gadget like jQuery, an attacker who convinces a victim to visit a specially crafted link could achieve arbitrary javascript execution	N/A	A-STR-STRI-170523/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the user's browser. **CVE ID : CVE-2023-2582**		
Vendor: struktur					
Product: libheif					
Affected Version(s): 1.15.1					
Divide By Zero	05-May-2023	6.5	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round () function in box.cc, which causes a denial of service. **CVE ID : CVE-2023-29659**	N/A	A-STR-LIBH-170523/774
Vendor: supportcandy					
Product: supportcandy					
Affected Version(s): * Up to (excluding) 3.1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	9.8	The SupportCandy WordPress plugin before 3.1.5 does not validate and escape user input before using it in an SQL statement, which could allow unauthenticated attackers to perform SQL injection attacks **CVE ID : CVE-2023-1730**	N/A	A-SUP-SUPP-170523/775
Vendor: surbma					
Product: gdpr_proof_cookie_consent_\&_notice_bar					
Affected Version(s): * Up to (excluding) 17.6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Surbma Surbma | GDPR Proof Cookie Consent & Notice Bar plugin <= 17.5.3 versions. **CVE ID : CVE-2023-23894**	N/A	A-SUR-GDPR-170523/776
Vendor: Suse					
Product: rancher					
Affected Version(s): From (including) 2.6.0 Up to (including) 2.7.2					
Improper Privilege Management	04-May-2023	9.9	Improper Privilege Management vulnerability in SUSE Rancher allows Privilege Escalation. A failure in the update logic of Rancher's admission Webhook may lead to the misconfiguration of the Webhook. This component enforces validation rules and security checks before resources are admitted into the Kubernetes cluster. The issue only affects users that upgrade from 2.6.x or 2.7.x to 2.7.2. Users that did a fresh install of 2.7.2 (and did not follow an upgrade path) are not affected.	https://bugzilla.suse.com/show_bug.cgi?id=CVE-2023-22651	A-SUS-RANC-170523/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22651		
Vendor: tapfiliate					
Product: tapfiliate					
Affected Version(s): * Up to (including) 3.0.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tapfiliate plugin <= 3.0.12 versions. **CVE ID : CVE-2023-25789**	N/A	A-TAP-TAPF-170523/778
Vendor: te-st					
Product: yandex.news_feed_by_teplitsa					
Affected Version(s): * Up to (excluding) 1.12.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Teplitsa Yandex.News Feed by Teplitsa plugin <= 1.12.5 versions. **CVE ID : CVE-2023-25052**	N/A	A-TE--YAND-170523/779
Vendor: Teampass					
Product: teampass					
Affected Version(s): * Up to (excluding) 3.0.7					
Improper Neutralization of Input During Web Page Generation	05-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.7.	https://github.com/nilsteampassnet/teampass/commit/39b774cba118ca5383b0a51a7	A-TEA-TEAM-170523/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-2516**	1b1e7dea2761927, https://hunter.dev/bounties/19470f0b-7094-4339-8d4a-4b5570b54716	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitHub repository nilsteampassnet/teampass prior to 3.0.7. **CVE ID : CVE-2023-2591**	https://hunter.dev/bounties/705f79f4-f5e3-41d7-82a5-f00441cd984b, https://github.com/nilsteampassnet/teampass/commit/57a977c6323656e5dc06ab5c227e75c3465a1a4a	A-TEA-TEAM-170523/781
Vendor: themeisle					
Product: visualizer					
Affected Version(s): * Up to (excluding) 3.9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Themeisle Visualizer: Tables and Charts Manager for WordPress plugin <= 3.9.4 versions. **CVE ID : CVE-2023-23708**	N/A	A-THE-VISU-170523/782
Vendor: timersys					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_popups					
Affected Version(s): * Up to (excluding) 2.1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	The WP Popups WordPress plugin before 2.1.5.1 does not properly escape the href attribute of its spu-facebook-page shortcode before outputting it 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. This is due to an insufficient fix of CVE-2023-24003 **CVE ID : CVE-2023-1905**	N/A	A-TIM-WP_P-170523/783
Vendor: Tipsandtricks-hq					
Product: category_specific_rss_feed_subscription					
Affected Version(s): * Up to (excluding) 2.2					
Cross-Site Request Forgery (CSRF)	03-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tips and Tricks HQ, Ruhul Amin Category Specific RSS feed Subscription plugin <= v2.1 versions. **CVE ID : CVE-2023-22691**	N/A	A-TIP-CATE-170523/784
Vendor: tms-outsource					
Product: wpdatatables					
Affected Version(s): * Up to (excluding) 2.1.50					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TMS-Plugins wpDataTables plugin <= 2.1.49 versions. **CVE ID : CVE-2023-23876**	N/A	A-TMS-WPDA-170523/785
Vendor: topdigitaltrends					
Product: mega_addons_for_wpbakery_page_builder					
Affected Version(s): * Up to (excluding) 4.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	The Mega Addons For WPBakery Page Builder WordPress plugin before 4.3.0 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-2023-0268**	N/A	A-TOP-MEGA-170523/786
Product: ultimate_carousel_for_elementor					
Affected Version(s): * Up to (including) 2.1.7					
Improper Neutralization of Input During Web Page Generation	08-May-2023	5.4	The Ultimate Carousel For Elementor WordPress plugin through 2.1.7 does not validate and escape some of its block options before	N/A	A-TOP-ULTI-170523/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-2023-0280**		
Product: ultimate_carousel_for_wpbakery_page_builder					
Affected Version(s): * Up to (including) 2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	5.4	The Ultimate Carousel For WPBakery Page Builder WordPress plugin through 2.6 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-2023-0267**	N/A	A-TOP-ULTI-170523/788
Vendor: tortall					
Product: yasm					
Affected Version(s): 1.3.0					
Missing Release of Memory after	09-May-2023	9.8	yasm v1.3.0 was discovered to contain a memory leak via the function yasm_intnum_copy	N/A	A-TOR-YASM-170523/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			at /libyasm/intnum.c. **CVE ID : CVE-2023-31975**		
Use After Free	09-May-2023	7.8	yasm v1.3.0 was discovered to contain a use after free via the function pp_getline at /nasm/nasm-pp.c. **CVE ID : CVE-2023-31972**	N/A	A-TOR-YASM-170523/790
Missing Release of Memory after Effective Lifetime	09-May-2023	7.8	yasm v1.3.0 was discovered to contain a use after free via the function expand_mmac_params at /nasm/nasm-pp.c. **CVE ID : CVE-2023-31973**	N/A	A-TOR-YASM-170523/791
Use After Free	09-May-2023	7.8	yasm v1.3.0 was discovered to contain a use after free via the function error at /nasm/nasm-pp.c. **CVE ID : CVE-2023-31974**	N/A	A-TOR-YASM-170523/792
Vendor: total-soft					
Product: video_gallery					
Affected Version(s): * Up to (excluding) 1.7.7					
Improper Neutralization of Input During Web Page Generation	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Video Gallery by Total-Soft Video Gallery plugin <= 1.7.6 versions.	N/A	A-TOT-VIDE-170523/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-25979**		
Vendor: totaljs					
Product: flow					
Affected Version(s): 10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS Flow v10 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the platform name field in the settings module. **CVE ID : CVE-2023-30094**	https://github.com/totaljs/flow/issues/100	A-TOT-FLOW-170523/794
Product: messenger					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the channel description field. **CVE ID : CVE-2023-30095**	https://github.com/totaljs/messenger/issues/11	A-TOT-MESS-170523/795
Improper Neutralization of Input During Web Page	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to	https://github.com/totaljs/messenger/issues/10	A-TOT-MESS-170523/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			execute arbitrary web scripts or HTML via a crafted payload injected into the user information field. **CVE ID : CVE-2023-30096**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in TotalJS messenger commit b6cf1c9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the private task field. **CVE ID : CVE-2023-30097**	https://github.com/totaljs/messenger/issues/9	A-TOT-MESS-170523/797
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 2.0.0					
Insertion of Sensitive Information into Log File	02-May-2023	5.5	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log. **CVE ID : CVE-2023-31207**	https://checkmk.com/werk/15189	A-TRI-CHEC-170523/798
Affected Version(s): 2.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	02-May-2023	5.5	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log. **CVE ID : CVE-2023-31207**	https://checkmk.com/werk/15189	A-TRI-CHEC-170523/799
Affected Version(s): 2.2.0					
Insertion of Sensitive Information into Log File	02-May-2023	5.5	Transmission of credentials within query parameters in Checkmk <= 2.1.0p26, <= 2.0.0p35, and <= 2.2.0b6 (beta) may cause the automation user's secret to be written to the site Apache access log. **CVE ID : CVE-2023-31207**	https://checkmk.com/werk/15189	A-TRI-CHEC-170523/800
Vendor: triton_project					
Product: triton					
Affected Version(s): * Up to (excluding) 3.7.5					
N/A	01-May-2023	9.8	Triton is a Minecraft plugin for Spigot and BungeeCord that helps you translate your Minecraft server. The CustomPayload packet allows you to execute commands	https://github.com/tritonmc/Triton/security/advisories/GHSA-8vj5-jccf-q25r	A-TRI-TRIT-170523/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the spigot/bukkit console. When you enable bungee mode in the config it will enable the bungee bridge and the server will begin to broadcast the 'triton:main' plugin channel. Using this plugin channel you are able to send a payload packet containing a byte (2) and a string (any spigot command). This could be used to make yourself a server operator and be used to extract other user information through phishing (pretending to be an admin), many servers use essentials so the /geoip command could be available to them, etc. This could also be modified to allow you to set the servers language, set another players language, etc. This issue affects those who have bungee enabled in config. This issue has been fixed in version 3.8.4. **CVE ID : CVE-2023-30859**		
Affected Version(s): From (including) 3.8.0 Up to (excluding) 3.8.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	9.8	Triton is a Minecraft plugin for Spigot and BungeeCord that helps you translate your Minecraft server. The CustomPayload packet allows you to execute commands on the spigot/bukkit console. When you enable bungee mode in the config it will enable the bungee bridge and the server will begin to broadcast the 'triton:main' plugin channel. Using this plugin channel you are able to send a payload packet containing a byte (2) and a string (any spigot command). This could be used to make yourself a server operator and be used to extract other user information through phishing (pretending to be an admin), many servers use essentials so the /geoip command could be available to them, etc. This could also be modified to allow you to set the servers language, set another players language, etc. This issue affects those	https://github.com/tritonmc/Triton/security/advisories/GHSA-8vj5-jccf-q25r	A-TRI-TRIT-170523/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			who have bungee enabled in config. This issue has been fixed in version 3.8.4. **CVE ID : CVE-2023-30859**		
Vendor: typecho					
Product: typecho					
Affected Version(s): * Up to (including) 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Typecho v1.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the url parameter at /index.php/archives/1/comment. **CVE ID : CVE-2023-30184**	N/A	A-TYP-TYPE-170523/803
Vendor: usbmemorydirect					
Product: simple_custom_author_profiles					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in USB Memory Direct Simple Custom Author Profiles plugin <= 1.0.0 versions. **CVE ID : CVE-2023-24372**	N/A	A-USB-SIMP-170523/804
Vendor: userlike					
Product: userlike					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David Voswinkel Userlike – WordPress Live Chat plugin <= 2.2 versions. **CVE ID : CVE-2023-23734**	N/A	A-USE-USER-170523/805
Vendor: vertical_scroll_recent_post_project					
Product: vertical_scroll_recent_post					
Affected Version(s): * Up to (including) 14.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Vertical scroll recent post plugin <= 14.0 versions. **CVE ID : CVE-2023-23862**	N/A	A-VER-VERT-170523/806
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.1532					
Integer Overflow or Wraparound	09-May-2023	7.8	Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.1532. **CVE ID : CVE-2023-2610**	https://github.com/vim/vim/commit/ab9a2d884b3a4abe319606ea95a5a6d6b01cd73a, https://huntr.dev/bounties/31e67340-935b-4f6c-a923-	A-VIM-VIM-170523/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				f7246bc29c7d	
Vendor: virtualreception					
Product: digital_reciptie					
Affected Version(s): win7sp1_rtm.101119-1850_6.1.7601.1.0.65792					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-May-2023	7.5	Directory Traversal vulnerability in virtualreception Digital Receptie version win7sp1_rtm.101119-1850 6.1.7601.1.0.65792 in embedded web server, allows attacker to gain sensitive information via a crafted GET request. **CVE ID : CVE-2023-25289**	N/A	A-VIR-DIGI-170523/808
Vendor: vk.company					
Product: mymail					
Affected Version(s): * Up to (including) 14.30					
Missing Encryption of Sensitive Data	07-May-2023	7.5	The myMail app through 14.30 for iOS sends cleartext credentials in a situation where STARTTLS is expected by a server. **CVE ID : CVE-2023-32290**	https://mailbox.org/en/post/mailbox-org-discovers-unencrypted-password-transmission-in-mymail	A-VK.-MYMA-170523/809
Vendor: vslider_multi_image_slider_project					
Product: vslider_multi_image_slider					
Affected Version(s): * Up to (including) 4.1.2					
Improper Neutralization of	03-May-2023	4.8	Auth. Stored Cross-Site Scripting (XSS) vulnerability in	N/A	A-VSL-VSLI-170523/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Mr.Vibe vSlider Multi Image Slider for WordPress plugin <= 4.1.2 versions. **CVE ID : CVE-2023-25797**		
Vendor: W3					
Product: webassembly					
Affected Version(s): 1.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	03-May-2023	5.5	An issue in the component hang.wasm of WebAssembly 1.0 causes an infinite loop. **CVE ID : CVE-2023-30300**	N/A	A-W3-WEBA-170523/811
Vendor: web_design_easy_sign_up_project					
Product: web_design_easy_sign_up					
Affected Version(s): * Up to (including) 3.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Andrew @ Geeenville Web Design Easy Sign Up plugin <= 3.4.1 versions. **CVE ID : CVE-2023-23701**	N/A	A-WEB-WEB_-170523/812
Vendor: winterchen					
Product: my-site					
Affected Version(s): * Up to (excluding) 2023-03-30					
Improper Neutralization of Input During	01-May-2023	5.4	Cross Site Scripting (XSS) vulnerability in WinterChenS my-site before commit 3f0423da6d5200c7a	https://github.com/WinterChenS/my-	A-WIN-MY-S-170523/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			46e200da145c1f54ee18548, allows attackers to inject arbitrary web script or HTML via editing blog articles. **CVE ID : CVE-2023-29638**	site/issues/74	
Vendor: winwar					
Product: wp_email_capture					
Affected Version(s): * Up to (excluding) 3.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media WP Email Capture plugin <= 3.9.3 versions. **CVE ID : CVE-2023-23723**	N/A	A-WIN-WP_E-170523/814
Vendor: wjjsoft					
Product: innokb					
Affected Version(s): 2.2.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-May-2023	7.5	WJJ Software - InnoKB Server, InnoKB/Console 2.2.1 - CWE-22: Path Traversal **CVE ID : CVE-2023-31181**	N/A	A-WJJ-INNO-170523/815
Improper Neutralization of Input During	08-May-2023	6.1	WJJ Software - InnoKB Server, InnoKB/Console	N/A	A-WJJ-INNO-170523/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			2.2.1 - Reflected cross-site scripting (RXSS) through an unspecified request. **CVE ID : CVE-2023-31180**		
Vendor: wpdownloadmanager					
Product: download_manager					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.3.0					
N/A	02-May-2023	7.5	The Download Manager WordPress plugin before 6.3.0 leaks master key information without the need for a password, allowing attackers to download arbitrary password-protected package files. **CVE ID : CVE-2023-1809**	N/A	A-WPD-DOWN-170523/817
Product: gutenberg_blocks_for_wordpress_download_manager					
Affected Version(s): * Up to (excluding) 2.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress Download Manager Gutenberg Blocks by WordPress Download Manager plugin <= 2.1.8 versions. **CVE ID : CVE-2023-22713**	N/A	A-WPD-GUTE-170523/818
Vendor: wpinventory					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_inventory_manager					
Affected Version(s): * Up to (excluding) 2.1.0.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	6.1	The WP Inventory Manager WordPress plugin before 2.1.0.12 does not sanitise and escape the message parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as administrators. **CVE ID : CVE-2023-1806**	N/A	A-WPI-WP_I-170523/819
Vendor: wpmart					
Product: team_member_-_team_with_slider					
Affected Version(s): * Up to (including) 4.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-May-2023	5.4	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in Sk. Abul Hasan Team Member – Team with Slider plugin <= 4.4 versions. **CVE ID : CVE-2023-23647**	N/A	A-WPM-TEAM-170523/820
Vendor: wpmobile.app_project					
Product: wpmobile.app					
Affected Version(s): * Up to (excluding) 11.19					
Improper Neutralization of Input During	04-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPMobile.App	N/A	A-WPM-WPMO-170523/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			plugin <= 11.18 versions. **CVE ID : CVE-2023-26010**		
Vendor: wpruby					
Product: ruby_help_desk					
Affected Version(s): * Up to (excluding) 1.3.4					
Authorization Bypass Through User-Controlled Key	02-May-2023	6.5	The Ruby Help Desk WordPress plugin before 1.3.4 does not ensure that the ticket being modified belongs to the user making the request, allowing an attacker to close and/or add files and replies to tickets other than their own. **CVE ID : CVE-2023-1125**	N/A	A-WPR-RUBY-170523/822
Vendor: wp_baidu_submit_project					
Product: wp_baidu_submit					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Include WP BaiDu Submit plugin <= 1.2.1 versions. **CVE ID : CVE-2023-25796**	N/A	A-WP_-WP_B-170523/823
Vendor: wp_content_filter_-_censor_all_offensive_content_from_your_site_project					
Product: wp_content_filter_-_censor_all_offensive_content_from_your_site					
Affected Version(s): * Up to (including) 3.0.1					
Improper Neutralization of	09-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS)	N/A	A-WP_-WP_C-170523/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerability in David Gwyer WP Content Filter plugin <= 3.0.1 versions. **CVE ID : CVE-2023-23883**		
Vendor: wp_custom_author_url_project					
Product: wp_custom_author_url					
Affected Version(s): * Up to (excluding) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	4.8	The WP Custom Author URL WordPress plugin before 1.0.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-1614**	N/A	A-WP_-WP_C-170523/825
Vendor: wp_login_box_project					
Product: wp_login_box					
Affected Version(s): * Up to (including) 2.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-May-2023	4.8	The WP Login Box WordPress plugin through 2.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting	N/A	A-WP_-WP_L-170523/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-0544**		
Vendor: wp_open_social_project					
Product: wp_open_social					
Affected Version(s): * Up to (including) 5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in XiaoMac WP Open Social plugin <= 5.0 versions. **CVE ID : CVE-2023-25792**	N/A	A-WP_-WP_O-170523/827
Vendor: wp_resource_download_management_project					
Product: wp_resource_download_management					
Affected Version(s): * Up to (including) 1.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wbolt team WP?????? plugin <= 1.3.9 versions. **CVE ID : CVE-2023-25787**	N/A	A-WP_-WP_R-170523/828
Vendor: wp_simple_events_project					
Product: wp_simple_events					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input	08-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nico	N/A	A-WP_-WP_S-170523/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Graff WP Simple Events plugin <= 1.0 versions. **CVE ID : CVE-2023-24376**		
Vendor: Zammad					
Product: Zammad					
Affected Version(s): From (including) 5.3.0 Up to (excluding) 5.4.0					
N/A	02-May-2023	6.5	Zammad 5.3.x (Fixed 5.4.0) is vulnerable to Incorrect Access Control. An authenticated attacker could gain information about linked accounts of users involved in their tickets using the Zammad API. **CVE ID : CVE-2023-29867**	https://zammad.com/en/advisories/zaa-2023-02	A-ZAM-ZAMM-170523/830
N/A	02-May-2023	6.5	Zammad 5.3.x (Fixed in 5.4.0) is vulnerable to Incorrect Access Control. An authenticated attacker with agent and customer roles could perform unauthorized changes on articles where they only have customer permissions. **CVE ID : CVE-2023-29868**	https://zammad.com/en/advisories/zaa-2023-01	A-ZAM-ZAMM-170523/831
Vendor: zhenfeng13_my-blog_project					
Product: zhenfeng13_my-blog					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	5.4	Cross site scripting (XSS) vulnerability in ZHENFENG13 My-Blog, allows attackers to inject arbitrary web script or HTML via the "title" field in the "blog management" page due to the the default configuration not using MyBlogUtils.cleanString. **CVE ID : CVE-2023-29636**	https://github.com/ZHENFENG13/My-Blog/issues/131	A-ZHE-ZHEN-170523/832
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	5.4	Cross site scripting (XSS) vulnerability in ZHENFENG13 My-Blog, allows attackers to inject arbitrary web script or HTML via editing an article in the "blog article" page due to the default configuration not utilizing MyBlogUtils.cleanString. **CVE ID : CVE-2023-29639**	https://github.com/ZHENFENG13/My-Blog/issues/131	A-ZHE-ZHEN-170523/833
Vendor: Zohocorp					
Product: manageengine_opmanager					
Affected Version(s): * Up to (excluding) 12.6					
N/A	04-May-2023	8.8	Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code	https://www.manageengine.com/network-monitoring/security-updates/cve-	A-ZOH-MANA-170523/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution via probe servers. **CVE ID : CVE-2023-31099**	2023-31099.html	
Affected Version(s): 12.6					
N/A	04-May-2023	8.8	Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code execution via probe servers. **CVE ID : CVE-2023-31099**	https://www.manageengine.com/network-monitoring/security-updates/cve-2023-31099.html	A-ZOH-MANA-170523/835
Vendor: zyrex					
Product: popup					
Affected Version(s): * Up to (excluding) 1.1					
Unrestricted Upload of File with Dangerous Type	02-May-2023	7.2	The ZYREX POPUP WordPress plugin through 1.0 does not validate the type of files uploaded when creating a popup, allowing a high privileged user (such as an Administrator) to upload arbitrary files, even when modifying the file system is disallowed, such as in a multisite install. **CVE ID : CVE-2023-0924**	N/A	A-ZYR-POPU-170523/836
Hardware					
Vendor: Advantech					
Product: eki-1521					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2573**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	H-ADV-EKI--170523/837
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2574**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	H-ADV-EKI--170523/838
Out-of-bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3,	H-ADV-EKI--170523/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2575**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	
Product: eki-1522					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2573**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	H-ADV-EKI--170523/840
Improper Neutralization of Special Elements used in a Command ('Comman	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/sup	H-ADV-EKI--170523/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			authenticated users via a crafted POST request. **CVE ID : CVE-2023-2574**	port/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	
Out-of-bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2575**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	H-ADV-EKI--170523/842
Product: eki-1524					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request.	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.	H-ADV-EKI--170523/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2573	com/en/support/details/firmware?id=1-1J9BEBL	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2574**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	H-ADV-EKI--170523/844
Out-of-bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2575**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	H-ADV-EKI--170523/845
Vendor: aigital					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wireless-n_repeater_mini_router					
Affected Version(s): -					
Insufficient Session Expiration	02-May-2023	7.5	An issue in the time-based authentication mechanism of Aigital Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to bypass login by connecting to the web app after a successful attempt by a legitimate user. **CVE ID : CVE-2023-30403**	N/A	H-AIG-WIRE-170523/846
Vendor: Amazon					
Product: fire_tv_stick_3rd_gen					
Affected Version(s): -					
Use of Insufficiently Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3.	N/A	H-AMA-FIRE-170523/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1385		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1384**	N/A	H-AMA-FIRE-170523/848
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServices function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5.	N/A	H-AMA-FIRE-170523/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1383**		
Vendor: Apple					
Product: studio_display					
Affected Version(s): -					
Out-of-bounds Write	08-May-2023	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27965**	https://support.apple.com/en-us/HT213672, https://support.apple.com/en-us/HT213670	H-APP-STUD-170523/850
Vendor: Asus					
Product: rt-ac51u					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.2	A Cross-site scripting (XSS) vulnerability in the System Log/General Log page of the administrator web UI in ASUS RT-AC51U wireless router firmware version up to and including 3.0.0.4.380.8591 allows remote attackers to inject arbitrary web script	N/A	H-ASU-RT-A-170523/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or HTML via a malicious network request. **CVE ID : CVE-2023-29772**		
Vendor: bestbuy					
Product: insignia_tv					
Affected Version(s): -					
Use of Insufficiently Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3. **CVE ID : CVE-2023-1385**	N/A	H-BES-INSI-170523/852
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run	N/A	H-BES-INSI-170523/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1384**		
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServices function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1383**	N/A	H-BES-INSI-170523/854
Vendor: Cisco					
Product: spa112					
Affected Version(s): -					
Missing Authentication for	04-May-2023	9.8	A vulnerability in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/	H-CIS-SPA1-170523/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with full privileges. Cisco has not released firmware updates to address this vulnerability. **CVE ID : CVE-2023-20126**	content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW	
Vendor: Dlink					
Product: dir-868l					
Affected Version(s): a1					
Buffer Copy without Checking Size of Input ('Classic	02-May-2023	9.8	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-868L Hardware version A1, firmware version 1.12 is vulnerable to Buffer Overflow. The	https://www.dlink.com/en/security-bulletin/, https://supportannouncement.us.dlin	H-DLI-DIR--170523/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			vulnerability is in scandir.sgi binary. **CVE ID : CVE-2023-29856**	k.com/announcement/publication.aspx?name=SAP10325	
Product: dir-879					
Affected Version(s): a1					
Improper Authentication	01-May-2023	7.5	D-Link DIR-879 v105A1 is vulnerable to Authentication Bypass via phpcgi. **CVE ID : CVE-2023-30061**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--170523/857
Product: dir-890l					
Affected Version(s): a1					
Improper Authentication	01-May-2023	7.5	D-Link DIR-890L FW1.10 A1 is vulnerable to Authentication bypass. **CVE ID : CVE-2023-30063**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--170523/858
Vendor: ez-net					
Product: next-7004n					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	6.1	A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affected is an unknown function of the file /boafrm/formFilter of the component POST Request Handler. The manipulation of the argument url with the input <svg	N/A	H-EZ--NEXT-170523/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			onload=alert(1337)> leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-228012. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2521**		
Vendor: feiyuxing					
Product: vec40g					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-May-2023	7.2	A vulnerability was found in Chengdu VEC40G 3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /send_order.cgi?parameter=access_detect of the component Network Detection. The manipulation of the argument COUNT with the input 3 | netstat -an leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	H-FEI-VEC4-170523/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier VDB-228013 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2522**		
Vendor: fiio					
Product: m6					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.8	A buffer overflow in the component /proc/ftxxxx-debug of FiiO M6 Build Number v1.0.4 allows attackers to escalate privileges to root. **CVE ID : CVE-2023-30257**	N/A	H-FII-M6-170523/861
Vendor: garo					
Product: wallbox_glb					
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack. **CVE ID : CVE-2023-30399**	N/A	H-GAR-WALL-170523/862
Product: wallbox_gtb					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack. **CVE ID : CVE-2023-30399**	N/A	H-GAR-WALL-170523/863
Product: wallbox_gtc					
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack. **CVE ID : CVE-2023-30399**	N/A	H-GAR-WALL-170523/864
Vendor: gl-inet					
Product: gl-mt3000					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	02-May-2023	9.8	GL.iNET MT3000 4.1.0 Release 2 is vulnerable to OS Command Injection via /usr/lib/oui-httpd/rpc/logread. **CVE ID : CVE-2023-29778**	N/A	H-GL--GL-M-170523/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Vendor: H3C					
Product: gr-1200w					
Affected Version(s): -					
Out-of-bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function set_tftp_upgrad. **CVE ID : CVE-2023-29693**	N/A	H-H3C-GR-1-170523/866
Out-of-bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function version_set. **CVE ID : CVE-2023-29696**	N/A	H-H3C-GR-1-170523/867
Vendor: HP					
Product: integrated_lights-out					
Affected Version(s): 6					
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04472en_us	H-HP-INTE-170523/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28092		
Product: proliant_rl300					
Affected Version(s): gen_11					
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis. **CVE ID : CVE-2023-28092**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04472en_us	H-HP-PROL-170523/869
Vendor: IBM					
Product: 3948-ved					
Affected Version(s): -					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	H-IBM-3948-170523/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 3957-vec					
Affected Version(s): -					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	H-IBM-3957-170523/871
Product: 3957-ved					
Affected Version(s): -					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	H-IBM-3957-170523/872
Vendor: Lenovo					
Product: smart_clock_essential_with_alexa_built_in					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	01-May-2023	8.8	A default password was reported in Lenovo Smart Clock Essential with Alexa Built In that could allow unauthorized device access to an attacker with local network access. **CVE ID : CVE-2023-0896**	https://support.lenovo.com/us/en/product_security/LEN-113714	H-LEN-SMAR-170523/873
Product: thinkagile_hx1021					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/874
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/875
Product: thinkagile_hx1320					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/876
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/877
Product: thinkagile_hx1321					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/878
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx1331					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/880
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/881
Product: thinkagile_hx1520-r					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/883
Product: thinkagile_hx1521-r					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/884
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx2320-e					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/886
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/887
Product: thinkagile_hx2321					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/888
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_hx2330					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/890
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/891
Product: thinkagile_hx2331					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/892
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/893
Product: thinkagile_hx2720-e					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/894
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx3320					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/896
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/897
Product: thinkagile_hx3321					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/899
Product: thinkagile_hx3330					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/900
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx3331					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/902
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/903
Product: thinkagile_hx3375					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/904
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_hx3376					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/906
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/907
Product: thinkagile_hx3520-g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/908
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/909
Product: thinkagile_hx3521-g					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/910
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx3720					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/912
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/913
Product: thinkagile_hx3721					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/915
Product: thinkagile_hx5520					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/916
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx5520-c					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/918
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/919
Product: thinkagile_hx5521					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/920
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_hx5521-c					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/922
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/923
Product: thinkagile_hx5530					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/924
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/925
Product: thinkagile_hx5531					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/926
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx7520					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/928
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/929
Product: thinkagile_hx7521					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/931
Product: thinkagile_hx7530					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/932
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx7531					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/934
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/935
Product: thinkagile_hx7820					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/936
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_hx7821					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/938
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/939
Product: thinkagile_hx_enclosure					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/940
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/941
Product: thinkagile_mx1020					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/942
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_mx1021_on_se350					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/944
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/945
Product: thinkagile_mx3330-f					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/947
Product: thinkagile_mx3330-h					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/948
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_mx3331-f					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/950
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/951
Product: thinkagile_mx3331-h					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/952
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_mx3530-h					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/954
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/955
Product: thinkagile_mx3530_f					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/956
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/957
Product: thinkagile_mx3531-f					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/958
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_mx3531_h					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/960
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/961
Product: thinkagile_vx1320					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/963
Product: thinkagile_vx2320					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/964
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_vx2330					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/966
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/967
Product: thinkagile_vx3320					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/968
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_vx3330					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/970
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/971
Product: thinkagile_vx3331					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/972
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/973
Product: thinkagile_vx3520-g					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/974
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_vx3530-g					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/976
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/977
Product: thinkagile_vx3720					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/979
Product: thinkagile_vx5520					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/980
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_vx5530					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/982
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/983
Product: thinkagile_vx7320_n					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/984
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_vx7330					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/986
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/987
Product: thinkagile_vx7520					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/988
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/989
Product: thinkagile_vx7520_n					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/990
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_vx7530					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/992
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/993
Product: thinkagile_vx7531					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/995
Product: thinkagile_vx7820					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/996
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_vx_1se					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/998
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/999
Product: thinkagile_vx_2u4n					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1000
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_vx_4u					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1002
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1003
Product: thinkedge_se450_					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1004
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1005
Product: thinkstation_p920					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1006
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sd530					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1008
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1009
Product: thinksystem_sd630_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1011
Product: thinksystem_sd650					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1012
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sd650-n_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1014
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1015
Product: thinksystem_sd650_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1016
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_se350					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1018
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1019
Product: thinksystem_sn550					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1020
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1021
Product: thinksystem_sn550_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1022
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sn850					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1024
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1025
Product: thinksystem_sr150					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1027
Product: thinksystem_sr158					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1028
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sr250					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1030
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1031
Product: thinksystem_sr250_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1032
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sr258					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1034
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1035
Product: thinksystem_sr258_v2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1036
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1037
Product: thinksystem_sr530					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1038
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sr550					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1040
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1041
Product: thinksystem_sr570					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1043
Product: thinksystem_sr590					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1044
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sr630					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1046
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1047
Product: thinksystem_sr630_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1048
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sr645					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1050
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1051
Product: thinksystem_sr645_v3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1052
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1053
Product: thinksystem_sr650					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1054
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sr650_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1056
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1057
Product: thinksystem_sr665					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1059
Product: thinksystem_sr665_v3					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1060
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sr670					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1062
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1063
Product: thinksystem_sr670_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1064
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sr850					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1066
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1067
Product: thinksystem_sr850p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1068
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1069
Product: thinksystem_sr850_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1070
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sr860					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1072
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1073
Product: thinksystem_sr860_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1075
Product: thinksystem_sr950					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1076
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_st250					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1078
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1079
Product: thinksystem_st250_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1080
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	H-LEN-THIN-170523/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_st258					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1082
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1083
Product: thinksystem_st258_v2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1084
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1085
Product: thinksystem_st550					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1086
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_st650_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1088
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1089
Product: thinksystem_st658_v2					
Affected Version(s): -					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	H-LEN-THIN-170523/1091
Vendor: milesight					
Product: ncr\/camera					
Affected Version(s): -					
N/A	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 discloses sensitive information through an unspecified request. **CVE ID : CVE-2023-24505**	N/A	H-MIL-NCR\-170523/1092
Insufficiently Protected Credentials	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 exposes credentials through	N/A	H-MIL-NCR\-170523/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unspecified request. **CVE ID : CVE-2023-24506**		
Vendor: mitrastar					
Product: gpt-2741gnac-n2					
Affected Version(s): -					
N/A	05-May-2023	8.8	MitraStar GPT-2741GNAC-N2 with firmware BR_g5.9_1.11(WVK.0)b32 was discovered to contain a remote code execution (RCE) vulnerability in the ping function. **CVE ID : CVE-2023-30065**	N/A	H-MIT-GPT--170523/1094
Vendor: Qualcomm					
Product: 315_5g_iot_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-315_-170523/1095
Product: 8905					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/compa	H-QUA-8905-170523/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	ny/product-security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8905-170523/1097
Product: 8909					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8909-170523/1098
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8909-170523/1099
Product: 8917					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8917-170523/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8917-170523/1101
Product: 8952					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8952-170523/1102
Product: 8953					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8953-170523/1103
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8953-170523/1104
Product: 8953pro					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8953-170523/1105
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8953-170523/1106
Product: 8956					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8956-170523/1107
Product: 8976					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8976-170523/1108
Product: 8976pro					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8976-170523/1109
Product: 8998					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8998-170523/1110
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-8998-170523/1111
Product: 9206_lte_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-9206-170523/1112
Product: apq5053-aa					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ5-170523/1113
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ5-170523/1114
Product: apq8017					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1115
Product: apq8052					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1116
Product: apq8053-aa					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1117
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1118
Product: apq8053-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1119
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1120
Product: apq8053-lite					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	H-QUA-APQ8-170523/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1122
Product: apq8056					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1123
Product: apq8064au					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-APQ8-170523/1124
Product: apq8076					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-APQ8-170523/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: aqt1000					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-AQT1-170523/1126
Product: ar8031					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-AR80-170523/1127
Product: ar8035					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-AR80-170523/1128
Product: c-v2x_9150					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-C-V2-170523/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: csra6620					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-CSRA-170523/1130
Product: csra6640					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-CSRA-170523/1131
Product: csrb31024					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-CSRB-170523/1132
Product: flight_rb5_5g_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-FLIG-170523/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-FLIG-170523/1134
Product: home_hub_100_platform					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-HOME-170523/1135
Product: mdm9250					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MDM9-170523/1136
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MDM9-170523/1137
Product: mdm9628					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MDM9-170523/1138
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MDM9-170523/1139
Product: mdm9650					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MDM9-170523/1140
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MDM9-170523/1141
Product: msm8108					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	H-QUA-MSM8-170523/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1143
Product: msm8209					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1144
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1145
Product: msm8608					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1147
Product: msm8909w					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1148
Product: msm8996au					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-MSM8-170523/1149
Product: qam8295p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QAM8-170523/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QAM8-170523/1151
Product: qca-4020-0-217msp					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA--170523/1152
Product: qca-4020-1-217msp					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA--170523/1153
Product: qca-4024-0-68cmqfn					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA--170523/1154
Product: qca-4024-1-68cmqfn					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA--170523/1155
Product: qca6174					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1156
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1157
Product: qca6174a					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1158
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-170523/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: qca6310					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1160
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1161
Product: qca6320					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1162
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1163
Product: qca6335					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1164
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1165
Product: qca6390					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1166
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1167
Product: qca6391					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-QCA6-170523/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1169
Product: qca6420					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1170
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1171
Product: qca6421					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1173
Product: qca6426					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1174
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1175
Product: qca6430					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1176
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-170523/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: qca6431					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1178
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1179
Product: qca6436					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1180
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1181
Product: qca6564					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1182
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1183
Product: qca6564a					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1184
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1185
Product: qca6564au					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-QCA6-170523/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1187
Product: qca6574					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1188
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1189
Product: qca6574a					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1191
Product: qca6574au					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1192
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1193
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1194
Product: qca6584au					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-170523/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	etins/may-2023-bulletin	
Product: qca6595					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1196
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1197
Product: qca6595au					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1198
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1199
Product: qca6696					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1200
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1201
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1202
Product: qca6698aq					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA6-170523/1203
Product: qca8081					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/compa	H-QUA-QCA8-170523/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	ny/product-security/bulletins/may-2023-bulletin	
Product: qca8337					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA8-170523/1205
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA8-170523/1206
Product: qca9367					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA9-170523/1207
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA9-170523/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9377					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA9-170523/1209
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA9-170523/1210
Product: qca9379					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA9-170523/1211
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCA9-170523/1212
Product: qcm2290					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCM2-170523/1213
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCM2-170523/1214
Product: qcm4290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCM4-170523/1215
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCM4-170523/1216
Product: qcm6125					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCM6-170523/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCM6-170523/1218
Product: qcm6490					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCM6-170523/1219
Product: qcn6024					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN6-170523/1220
Product: qcn9011					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCN9-170523/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN9-170523/1222
Product: qcn9012					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN9-170523/1223
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN9-170523/1224
Product: qcn9024					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN9-170523/1225
Product: qcn9074					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN9-170523/1226
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCN9-170523/1227
Product: qcs2290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS2-170523/1228
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS2-170523/1229
Product: qcs400					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCS4-170523/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Product: qcs410					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS4-170523/1231
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS4-170523/1232
Product: qcs4290					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS4-170523/1233
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS4-170523/1234
Product: qcs605					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS6-170523/1235
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS6-170523/1236
Product: qcs610					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS6-170523/1237
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS6-170523/1238
Product: qcs6125					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-QCS6-170523/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS6-170523/1240
Product: qcs6490					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS6-170523/1241
Product: qcs8155					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS8-170523/1242
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS8-170523/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8250					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS8-170523/1244
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QCS8-170523/1245
Product: qm215					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QM21-170523/1246
Product: qrb5165					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QRB5-170523/1247
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	H-QUA-QRB5-170523/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: qrb5165m					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QRB5-170523/1249
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QRB5-170523/1250
Product: qrb5165n					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QRB5-170523/1251
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QRB5-170523/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: qsm8250					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QSM8-170523/1253
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-QSM8-170523/1254
Product: sa4150p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA41-170523/1255
Product: sa4155p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA41-170523/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa6145p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1257
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1258
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1259
Product: sa6150p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1260
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SA61-170523/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1262
Product: sa6155					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1263
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1264
Product: sa6155p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1266
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA61-170523/1267
Product: sa8145p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1268
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1269
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SA81-170523/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: sa8150p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1271
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1272
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1273
Product: sa8155					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1274
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	H-QUA-SA81-170523/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: sa8155p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1276
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1277
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1278
Product: sa8195p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address.	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SA81-170523/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21642	2023-bulletin	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1280
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA81-170523/1281
Product: sa8295p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA82-170523/1282
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA82-170523/1283
Product: sa8540p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory	https://www.qualcomm	H-QUA-SA85-170523/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: sa9000p					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SA90-170523/1285
Product: sd626					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD62-170523/1286
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD62-170523/1287
Product: sd660					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-SD66-170523/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD66-170523/1289
Product: sd670					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD67-170523/1290
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD67-170523/1291
Product: sd675					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD67-170523/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD67-170523/1293
Product: sd730					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD73-170523/1294
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD73-170523/1295
Product: sd835					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD83-170523/1296
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SD83-170523/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: sd855					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD85-170523/1298
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD85-170523/1299
Product: sd865_5g					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD86-170523/1300
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD86-170523/1301
Product: sd888					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD88-170523/1302
Product: sda\/sdm845					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDA\-170523/1303
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDA\-170523/1304
Product: sdm429					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1305
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer	https://www.qualcomm.com/company/product-	H-QUA-SDM4-170523/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			allocated through the graphics pool. **CVE ID : CVE-2023-21666**	security/bulletins/may-2023-bulletin	
Product: sdm429w					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1307
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1308
Product: sdm439					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1309
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sdm450					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1311
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM4-170523/1312
Product: sdm660					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM6-170523/1313
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM6-170523/1314
Product: sdm670					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM6-170523/1315
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM6-170523/1316
Product: sdm710					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM7-170523/1317
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM7-170523/1318
Product: sdm845					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDM8-170523/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDM8-170523/1320
Product: sdx20m					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDX2-170523/1321
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDX2-170523/1322
Product: sdx55					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDX5-170523/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SDX5-170523/1324
Product: sd_675					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD_6-170523/1325
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SD_6-170523/1326
Product: sm4125					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM41-170523/1327
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM41-170523/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: sm4250-aa					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM42-170523/1329
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM42-170523/1330
Product: sm4350					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM43-170523/1331
Product: sm4350-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SM43-170523/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: sm4375					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM43-170523/1333
Product: sm6115					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1334
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1335
Product: sm6125					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1337
Product: sm6150					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1338
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1339
Product: sm6150-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM61-170523/1340
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM61-170523/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: sm6225					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1342
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1343
Product: sm6225-ad					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1344
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1345
Product: sm6250					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1346
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1347
Product: sm6250p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1348
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM62-170523/1349
Product: sm6350					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-SM63-170523/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM63-170523/1351
Product: sm6375					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM63-170523/1352
Product: sm7125					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1353
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm7150-aa					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1355
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1356
Product: sm7150-ab					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1357
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1358
Product: sm7150-ac					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1359
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM71-170523/1360
Product: sm7225					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1361
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1362
Product: sm7250-aa					
Affected Version(s): -					
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM72-170523/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: sm7250-ab					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1364
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1365
Product: sm7250-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1366
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1367
Product: sm7250p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1368
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM72-170523/1369
Product: sm7315					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM73-170523/1370
Product: sm7325					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM73-170523/1371
Product: sm7325-ae					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM73-170523/1372
Product: sm7325-af					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM73-170523/1373
Product: sm7325p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM73-170523/1374
Product: sm7350-ab					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM73-170523/1375
Product: sm8150					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM81-170523/1376
Product: sm8150-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM81-170523/1377
Product: sm8250					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM82-170523/1378
Product: sm8250-ab					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM82-170523/1379
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	H-QUA-SM82-170523/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: sm8250-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM82-170523/1381
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM82-170523/1382
Product: sm8350					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SM83-170523/1383
Product: sm8350-ac					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-SM83-170523/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	security/bulletins/may-2023-bulletin	
Product: snapdragon_1200_wearable_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1385
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1386
Product: snapdragon_208_processor					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1387
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_630_mobile_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1389
Product: snapdragon_632_mobile_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1390
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1391
Product: snapdragon_636_mobile_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1392
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1393
Product: snapdragon_820_automotive_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1394
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1395
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1396
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-170523/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1398
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1399
Product: snapdragon_w5\+_gen_1_wearable_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1400
Product: snapdragon_wear_2100_platform					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SNAP-170523/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: snapdragon_wear_2500_platform					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1402
Product: snapdragon_wear_3100_platform					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1403
Product: snapdragon_wear_4100\+_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1404
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_x12_lte_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1406
Product: snapdragon_x20_lte_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1407
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1408
Product: snapdragon_x24_lte_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1409
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	H-QUA-SNAP-170523/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1411
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1412
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1413
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SNAP-170523/1414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: snapdragon_x5_lte_modem					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1415
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1416
Product: snapdragon_x65_5g_modem-rf_system					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1417
Product: snapdragon_xr1_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1419
Product: snapdragon_xr2\+_gen_1_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1420
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1421
Product: snapdragon_xr2_5g_platform					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SNAP-170523/1422
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SNAP-170523/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: ssm7250-aa					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SSM7-170523/1424
Product: sw5100					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SW51-170523/1425
Product: sw5100p					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SW51-170523/1426
Product: sxr1120					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-security/bull	H-QUA-SXR1-170523/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SXR1-170523/1428
Product: sxr2130					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SXR2-170523/1429
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-SXR2-170523/1430
Product: wcd9326					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1432
Product: wcd9330					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1433
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1434
Product: wcd9335					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1435
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-170523/1436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: wcd9340					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1437
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1438
Product: wcd9341					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1439
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1440
Product: wcd9370					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1441
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1442
Product: wcd9371					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1443
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1444
Product: wcd9375					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-WCD9-170523/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1446
Product: wcd9380					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1447
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1448
Product: wcd9385					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCD9-170523/1450
Product: wcn3610					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1451
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1452
Product: wcn3615					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1453
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-170523/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: wcn3620					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1455
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1456
Product: wcn3660					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1457
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1458
Product: wcn3660b					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1459
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1460
Product: wcn3680					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1461
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1462
Product: wcn3680b					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	H-QUA-WCN3-170523/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1464
Product: wcn3910					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1465
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1466
Product: wcn3950					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1468
Product: wcn3980					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1469
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1470
Product: wcn3988					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1471
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCN3-170523/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: wcn3990					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1473
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1474
Product: wcn3998					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1475
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1476
Product: wcn3999					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1477
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN3-170523/1478
Product: wcn6740					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN6-170523/1479
Product: wcn6750					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN6-170523/1480
Product: wcn685x-1					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN6-170523/1481
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN6-170523/1482
Product: wcn685x-5					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN6-170523/1483
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WCN6-170523/1484
Product: wsa8810					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	H-QUA-WSA8-170523/1485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1486
Product: wsa8815					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1487
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1488
Product: wsa8830					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1490
Product: wsa8835					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1491
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	H-QUA-WSA8-170523/1492
Vendor: Rockwellautomation					
Product: armorstart_st_281e					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29030**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29031**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1494
Improper Neutralization of Input During	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell	https://rockwellautomation.custhelp.com/app/answers/answe	H-ROC-ARMO-170523/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Automation's ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29024**	r_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29023**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29022**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1497
Improper Neutralization of	11-May-2023	5.9		https://rockwellautomation.custhelp.c	H-ROC-ARMO-170523/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29025**	om/app/answers/answer_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29026**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29027		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29028**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1501
Improper Neutralization of Input	11-May-2023	5.9	A cross site scripting vulnerability was discovered in	https://rockwellautomation.custhelp.com/app/ans	H-ROC-ARMO-170523/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29029**	wers/answer_view/a_id/1139438	
Product: armorstart_st_284ee					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29030**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29031**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1504
Improper Neutralization of Input During Web Page	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell Automation's	https://rockwellautomation.custhelp.com/app/answers/answe	H-ROC-ARMO-170523/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29024**	r_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploitation of this vulnerability. **CVE ID : CVE-2023-29023**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29022**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1507
Improper Neutralization of Input	11-May-2023	5.9	A cross site scripting vulnerability was	https://rockwellautomation.custhelp.com/app/ans	H-ROC-ARMO-170523/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29025**	wers/answer_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29026**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29027		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29028**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1511
Improper Neutralization of Input During Web Page Generation	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	H-ROC-ARMO-170523/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29029**		
Vendor: Samsung					
Product: exynos					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21494**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	H-SAM-EXYN-170523/1513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_LteInterRatManagement.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21503**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	H-SAM-EXYN-170523/1514
Product: exynos_1080					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-170523/1515
Product: exynos_5123					
Affected Version(s): -					
Improper Handling of Exceptiona	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem	https://semiconductor.samsung.com/support/quality-	H-SAM-EXYN-170523/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**	support/product-security-updates/	
Product: exynos_5300					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-170523/1517
Product: exynos_980					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos	https://semiconductor.samsung.com/support/quality-support/pro	H-SAM-EXYN-170523/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**	duct-security-updates/	
Vendor: shapeshift					
Product: keepkey					
Affected Version(s): -					
Out-of-bounds Read	02-May-2023	5.7	Insufficient length checks in the ShapeShift KeepKey hardware wallet firmware before 7.7.0 allow a global buffer overflow via crafted messages. Flaws in cf_confirmExecTx() in ethereum_contracts.c can be used to reveal arbitrary microcontroller memory on the device screen or crash the device. With physical access to a PIN-unlocked device, attackers can extract the BIP39 mnemonic secret from the hardware wallet. **CVE ID : CVE-2023-27892**	https://github.com/keepkey/keepkey-firmware/pull/337	H-SHA-KEEP-170523/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Siemens					
Product: 6gk1411-1ac00					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to. **CVE ID : CVE-2023-29104**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1520
Missing Standardized Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). **CVE ID : CVE-2023-29105**		
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint.	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29106		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges. **CVE ID : CVE-2023-28832**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1523
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information resources. **CVE ID : CVE-2023-29107**		
Use of Hard-coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. **CVE ID : CVE-2023-29103**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1525
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`. **CVE ID : CVE-2023-29128**		
Product: 6gk1411-5ac00					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to.	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29104		
Missing Standardized Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). **CVE ID : CVE-2023-29105**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1528
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint. **CVE ID : CVE-2023-29106**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges. **CVE ID : CVE-2023-28832**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1530
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources. **CVE ID : CVE-2023-29107**		
Use of Hard-coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. **CVE ID : CVE-2023-29103**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	H-SIE-6GK1-170523/1532
Improper Limitation of a Pathname	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All	https://cert-portal.siemens.com/productcert/pdf/	H-SIE-6GK1-170523/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`. **CVE ID : CVE-2023-29128**	ssa-555292.pdf	
Product: scalance_lpe9403					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-May-2023	9.9	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user.	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	H-SIE-SCAL-170523/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27407		
Creation of Temporary File With Insecure Permissions	09-May-2023	3.3	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The `i2c` mutex file is created with the permissions bits of `-rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects. **CVE ID : CVE-2023-27408**	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	H-SIE-SCAL-170523/1535
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	3.3	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`.	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	H-SIE-SCAL-170523/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27409		
Heap-based Buffer Overflow	09-May-2023	2.7	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service. **CVE ID : CVE-2023-27410**	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	H-SIE-SCAL-170523/1537
Vendor: Tenda					
Product: ac18					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-May-2023	9.8	Tenda AC18 v15.03.05.19(6318_)_cn was discovered to contain a command injection vulnerability via the deviceName parameter in the setUsbUnload function. **CVE ID : CVE-2023-30135**	https://github.com/DrizzlingSun/Tenda/blob/main/AC18/8/8.md	H-TEN-AC18-170523/1538
Product: n301					
Affected Version(s): 6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	01-May-2023	5.7	Cleartext Transmission in set-cookie:ecos_pw: Tenda N301 v6.0, Firmware v12.02.01.61_multi allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password. **CVE ID : CVE-2023-29680**	N/A	H-TEN-N301-170523/1539
Cleartext Transmission of Sensitive Information	01-May-2023	5.7	Cleartext Transmission in cookie:ecos_pw: in Tenda N301 v6.0, firmware v12.03.01.06_pt allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password. **CVE ID : CVE-2023-29681**	N/A	H-TEN-N301-170523/1540
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191024 is vulnerable to Command Injection. **CVE ID : CVE-2023-30053**	N/A	H-TOT-A710-170523/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191024 has a Command Injection vulnerability. An attacker can obtain a stable root shell through a specially constructed payload. **CVE ID : CVE-2023-30054**	N/A	H-TOT-A710-170523/1542
Product: x5000r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and V9.1.0u.6369_B20230113 contain a command insertion vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary commands through the "command" parameter. **CVE ID : CVE-2023-30013**	N/A	H-TOT-X500-170523/1543
Vendor: Zyxel					
Product: Nbg-418n					
Affected Version(s): v2					
Improper Neutralization of Input During Web Page	01-May-2023	7.5	A cross-site scripting (XSS) vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0	https://www.zyxel.com/global/en/support/security-advisories/z	H-ZYX-NBG--170523/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			could allow a remote authenticated attacker with administrator privileges to store malicious scripts using a web management interface parameter, resulting in denial-of-service (DoS) conditions on an affected device. **CVE ID : CVE-2023-22921**	yxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-May-2023	7.5	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote unauthenticated attacker to cause DoS conditions by sending crafted packets if Telnet is enabled on a vulnerable device. **CVE ID : CVE-2023-22922**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	H-ZYX-NBG--170523/1545
Use of Externally-Controlled Format String	01-May-2023	6.5	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker to cause denial-of-service	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-	H-ZYX-NBG--170523/1546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) conditions on an affected device. **CVE ID : CVE-2023-22923**	418n-v2-home-router	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-May-2023	4.9	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing crafted CLI commands on a vulnerable device. **CVE ID : CVE-2023-22924**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	H-ZYX-NBG--170523/1547
Product: nbg6604					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-May-2023	8.8	The post-authentication command injection vulnerability in the Zyxel NBG6604 firmware version V1.01(ABIR.0)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request. **CVE ID : CVE-2023-22919**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-nbg6604-home-router	H-ZYX-NBG6-170523/1548
Operating System					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Advantech					
Product: eki-1521_firmware					
Affected Version(s): * Up to (including) 1.21					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2573**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	O-ADV-EKI--170523/1549
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2574**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	O-ADV-EKI--170523/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2575**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	O-ADV-EKI--170523/1551
Product: eki-1522_firmware					
Affected Version(s): * Up to (including) 1.21					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2573**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	O-ADV-EKI--170523/1552
Improper Neutralization of	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21	https://www.advantech.com/en/sup	O-ADV-EKI--170523/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2574**	port/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	
Out-of-bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2575**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	O-ADV-EKI--170523/1554
Product: eki-1524_firmware					
Affected Version(s): * Up to (including) 1.21					
Improper Neutralization of Special Elements used in a Command ('Comman	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the NTP server input field, which can be	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.	O-ADV-EKI--170523/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2573**	com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by an command injection vulnerability in the device name input field, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2574**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.com/en/support/details/firmware?id=1-1J9BEBL	O-ADV-EKI--170523/1556
Out-of-bounds Write	08-May-2023	8.8	Advantech EKI-1524, EKI-1522, EKI-1521 devices through 1.21 are affected by a Stack-based Buffer Overflow vulnerability, which can be triggered by authenticated users via a crafted POST request. **CVE ID : CVE-2023-2575**	https://www.advantech.com/en/support/details/firmware?id=1-1J9BED3, https://www.advantech.com/en/support/details/firmware?id=1-1J9BECT, https://www.advantech.	O-ADV-EKI--170523/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/en/support/details/firmware?id=1-1J9BEBL	
Vendor: aigital					
Product: wireless-n_repeater_mini_router_firmware					
Affected Version(s): 0.131229					
Insufficient Session Expiration	02-May-2023	7.5	An issue in the time-based authentication mechanism of Aigital Aigital Wireless-N Repeater Mini_Router v0.131229 allows attackers to bypass login by connecting to the web app after a successful attempt by a legitimate user. **CVE ID : CVE-2023-30403**	N/A	O-AIG-WIRE-170523/1558
Vendor: Amazon					
Product: fire_os					
Affected Version(s): * Up to (excluding) 6.2.9.5					
Use of Insufficiently Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects:	N/A	O-AMA-FIRE-170523/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3. **CVE ID : CVE-2023-1385**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1384**	N/A	O-AMA-FIRE-170523/1560
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServices function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible. This issue affects:	N/A	O-AMA-FIRE-170523/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1383**		
Affected Version(s): * Up to (excluding) 7.6.3.3					
Use of Insufficiently Random Values	03-May-2023	8.8	Improper JPAKE implementation allows offline PIN brute-forcing due to the initialization of random values to a known value, which leads to unauthorized authentication to amzn.lightning services. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS 7.6.3.3. **CVE ID : CVE-2023-1385**	N/A	O-AMA-FIRE-170523/1562
Improper Neutralization of Input During Web Page Generation	03-May-2023	6.1	The setMediaSource function on the amzn.thin.pl service does not sanitize the "source" parameter allowing for arbitrary javascript code to be run	N/A	O-AMA-FIRE-170523/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1384**		
N/A	03-May-2023	4.3	An Improper Enforcement of Behavioral Workflow vulnerability in the exchangeDeviceServices function on the amzn.dmgr service allowed an attacker to register services that are only locally accessible. This issue affects: Amazon Fire TV Stick 3rd gen versions prior to 6.2.9.5. Insignia TV with FireOS versions prior to 7.6.3.3. **CVE ID : CVE-2023-1383**	N/A	O-AMA-FIRE-170523/1564
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 15.7.4					
N/A	08-May-2023	7.8	The issue was addressed with improved bounds	https://support.apple.com/en-	O-APP-IPAD-170523/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-23536**	us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory **CVE ID : CVE-2023-27936**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1566
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5,	https://support.apple.com/en-us/HT213674, https://support.apple.com	O-APP-IPAD-170523/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	m/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://supp	O-APP-IPAD-170523/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to disclose kernel memory **CVE ID : CVE-2023-27941**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/kb/HT213675	O-APP-IPAD-170523/1569
Affected Version(s): * Up to (excluding) 16.4					
N/A	08-May-2023	9.8	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper **CVE ID : CVE-2023-23526**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1570
N/A	08-May-2023	8.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be	https://support.apple.com/en-us/HT213670, https://support.apple.co	O-APP-IPAD-170523/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to break out of its sandbox **CVE ID : CVE-2023-23532**	m/en-us/HT213676	
N/A	08-May-2023	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges **CVE ID : CVE-2023-23525**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	O-APP-IPAD-170523/1572
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676,	O-APP-IPAD-170523/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27933**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1574
Out-of-bounds Read	08-May-2023	6.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23528		
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1576
Out-of-bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://supp	O-APP-IPAD-170523/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of process memory **CVE ID : CVE-2023-27929**	ort.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27931**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213604, https://support.apple.com/kb/HT213603	O-APP-IPAD-170523/1578
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3,	https://support.apple.com/en-us/HT213674, https://supp	O-APP-IPAD-170523/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy **CVE ID : CVE-2023-27932**	ort.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27942**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677,	O-APP-IPAD-170523/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/kb/HT213675	
N/A	08-May-2023	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied **CVE ID : CVE-2023-27943**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	5.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to cause a denial-of-service **CVE ID : CVE-2023-23494**	https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1582
N/A	08-May-2023	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through Visual Lookup **CVE ID : CVE-2023-23523**		
Affected Version(s): From (including) 16.0 Up to (excluding) 16.4					
N/A	08-May-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-23536**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	O-APP-IPAD-170523/1584
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT21367	O-APP-IPAD-170523/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1586
Product: ipad_os					
Affected Version(s): * Up to (excluding) 15.7.4					
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in	https://support.apple.com/en-us/HT213673,	O-APP-IPAD-170523/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-28201**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213676	
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27946**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1588
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-	O-APP-IPAD-170523/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27949**	us/HT213670, https://support.apple.com/en-us/HT213677	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1590
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT21367	O-APP-IPAD-170523/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user **CVE ID : CVE-2023-27963**	0, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-IPAD-170523/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676	
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1593
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://supp	O-APP-IPAD-170523/1594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27956	ort.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1595
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This	https://support.apple.com/en-us/HT21367	O-APP-IPAD-170523/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory **CVE ID : CVE-2023-28200**	5, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
Affected Version(s): * Up to (excluding) 16.4					
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27959**	https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1597
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27970**	https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-28181**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1599
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files **CVE ID : CVE-2023-27955**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1600
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation.	https://support.apple.com/en-	O-APP-IPAD-170523/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences **CVE ID : CVE-2023-28178**	us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	3.3	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to unexpectedly create a bookmark on the Home Screen **CVE ID : CVE-2023-28194**	https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1602
Affected Version(s): From (including) 16.0 Up to (excluding) 16.4					
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-28201**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-	O-APP-IPAD-170523/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1604
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://supp	O-APP-IPAD-170523/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without prompting the user **CVE ID : CVE-2023-27963**	ort.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPAD-170523/1606
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This	https://support.apple.com/en-us/HT21367	O-APP-IPAD-170523/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	5, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27956**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-IPAD-170523/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPAD-170523/1609
Product: iphone_os					
Affected Version(s): * Up to (excluding) 15.7.4					
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT21367	O-APP-IPHO-170523/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-28201**	0, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-23536**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	O-APP-IPHO-170523/1611
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-	O-APP-IPHO-170523/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or write kernel memory **CVE ID : CVE-2023-27936**	us/HT213670, https://support.apple.com/en-us/HT213677	
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27946**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-IPHO-170523/1613
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-IPHO-170523/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27949		
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1615
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://supp	O-APP-IPHO-170523/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without prompting the user **CVE ID : CVE-2023-27963**	ort.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1617
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This	https://support.apple.com/en-us/HT21367	O-APP-IPHO-170523/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	5, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-	O-APP-IPHO-170523/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1620
N/A	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to disclose kernel memory	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://supp	O-APP-IPHO-170523/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27941	ort.apple.com/kb/HT213675	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27956**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1622
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670,	O-APP-IPHO-170523/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory **CVE ID : CVE-2023-28200**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-IPHO-170523/1624
Affected Version(s): * Up to (excluding) 16.4					
N/A	08-May-2023	9.8	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is	https://support.apple.com/en-us/HT213670, https://support.apple.co	O-APP-IPHO-170523/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper **CVE ID : CVE-2023-23526**	m/en-us/HT213676	
N/A	08-May-2023	8.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to break out of its sandbox **CVE ID : CVE-2023-23532**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1626
N/A	08-May-2023	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges **CVE ID : CVE-2023-23525**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	O-APP-IPHO-170523/1627
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-	O-APP-IPHO-170523/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27959**	https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1629
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary	https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with kernel privileges **CVE ID : CVE-2023-27970**		
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-28181**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1631
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27933**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT21367	O-APP-IPHO-170523/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				6, https://support.apple.com/en-us/HT213677	
Out-of-bounds Read	08-May-2023	6.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory **CVE ID : CVE-2023-23528**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1633
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.co	O-APP-IPHO-170523/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Out-of-bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27929**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1635
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27931**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678,	O-APP-IPHO-170523/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213604, https://support.apple.com/kb/HT213603	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy **CVE ID : CVE-2023-27932**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1637
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3,	https://support.apple.com/en-us/HT213674,	O-APP-IPHO-170523/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27942**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677, https://support.apple.com/kb/HT213675	
N/A	08-May-2023	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied **CVE ID : CVE-2023-27943**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1639
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey	https://support.apple.com/en-us/HT213675, https://supp	O-APP-IPHO-170523/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files **CVE ID : CVE-2023-27955**	ort.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences **CVE ID : CVE-2023-28178**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPHO-170523/1641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	5.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to cause a denial-of-service **CVE ID : CVE-2023-23494**	https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup **CVE ID : CVE-2023-23523**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1643
N/A	08-May-2023	3.3	The issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4. An app may be able to unexpectedly create a bookmark on the Home Screen **CVE ID : CVE-2023-28194**	https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1644
Affected Version(s): From (including) 16.0 Up to (excluding) 16.4					
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-	O-APP-IPHO-170523/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or arbitrary code execution **CVE ID : CVE-2023-28201**	us/HT213671, https://support.apple.com/en-us/HT213676	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1646
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://supp	O-APP-IPHO-170523/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user **CVE ID : CVE-2023-27963**	ort.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-IPHO-170523/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676	
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-IPHO-170523/1649
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://supp	O-APP-IPHO-170523/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23535	ort.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-IPHO-170523/1651
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue	https://support.apple.com/en-us/HT21367	O-APP-IPHO-170523/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27956**	4, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-IPHO-170523/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676, https://support.apple.com/en-us/HT213677	
Product: macos					
Affected Version(s): -					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-22372**	https://my.f5.com/manage/s/article/K000132522	O-APP-MACO-170523/1654
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132539	O-APP-MACO-170523/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24461		
Affected Version(s): * Up to (excluding) 10.4.8					
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in GarageBand for macOS 10.4.8. Parsing a maliciously crafted MIDI file may lead to an unexpected application termination or arbitrary code execution **CVE ID : CVE-2023-27938**	https://support.apple.com/en-us/HT213650	O-APP-MACO-170523/1656
Affected Version(s): * Up to (excluding) 11.7.5					
N/A	08-May-2023	8.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27935**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1657
N/A	08-May-2023	8.6	This issue was addressed with a new entitlement. This issue is fixed in	https://support.apple.com/en-us/HT21367	O-APP-MACO-170523/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox **CVE ID : CVE-2023-27944**	5, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory **CVE ID : CVE-2023-27936**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1659
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/	O-APP-MACO-170523/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted plist may lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	m/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://supp	O-APP-MACO-170523/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23534**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1662
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://supp	O-APP-MACO-170523/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1664
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper **CVE ID : CVE-2023-27951**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-	O-APP-MACO-170523/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to view sensitive information **CVE ID : CVE-2023-28189**	https://support.apple.com/en-us/HT213670, https://support.apple.com/kb/HT213675	O-APP-MACO-170523/1666
Affected Version(s): * Up to (excluding) 12.6.4					
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27933**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1667
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in	https://support.apple.com/en-us/HT21367	O-APP-MACO-170523/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system **CVE ID : CVE-2023-23533**	0, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system **CVE ID : CVE-2023-23538**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1669
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27942**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-	O-APP-MACO-170523/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213677, https://support.apple.com/kb/HT213675	
Affected Version(s): * Up to (excluding) 13.3					
N/A	08-May-2023	9.8	This was addressed with additional checks by Gatekeeper on files downloaded from an iCloud shared-by-me folder. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. A file from an iCloud shared-by-me folder may be able to bypass Gatekeeper **CVE ID : CVE-2023-23526**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1671
N/A	08-May-2023	8.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to break out of its sandbox **CVE ID : CVE-2023-23532**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1672
Improper Initialization	08-May-2023	8.8	A memory initialization issue was addressed. This issue is fixed in macOS Ventura 13.3. A remote user may be able to cause unexpected app	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or arbitrary code execution **CVE ID : CVE-2023-27934**		
N/A	08-May-2023	7.8	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to gain root privileges **CVE ID : CVE-2023-23525**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	O-APP-MACO-170523/1674
N/A	08-May-2023	7.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-23536**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213675	O-APP-MACO-170523/1675
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS	https://support.apple.com/en-us/HT213674,	O-APP-MACO-170523/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-28181**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	6.5	A denial-of-service issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. A user in a privileged network position may be able to cause a denial-of-service **CVE ID : CVE-2023-28180**	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1677
Out-of-bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27929**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://supp	O-APP-MACO-170523/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27931**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213604, https://support.apple.com/kb/HT213603	O-APP-MACO-170523/1679
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://supp	O-APP-MACO-170523/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web content may bypass Same Origin Policy **CVE ID : CVE-2023-27932**	ort.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to disclose kernel memory **CVE ID : CVE-2023-27941**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/kb/HT213675	O-APP-MACO-170523/1681
N/A	08-May-2023	5.5	This issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Files downloaded from the internet may not have the quarantine flag applied **CVE ID : CVE-2023-27943**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	5.5	A privacy issue was addressed by moving sensitive data to a more secure location. This issue is fixed in macOS Ventura 13.3. An app may be able to access user-sensitive data **CVE ID : CVE-2023-28190**	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1683
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-May-2023	4.7	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.3. An app may bypass Gatekeeper checks **CVE ID : CVE-2023-27952**	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1684
N/A	08-May-2023	3.3	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. Photos belonging to the Hidden Photos Album could be viewed without authentication through Visual Lookup **CVE ID : CVE-2023-23523**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1685
Affected Version(s): From (including) 11.0 Up to (excluding) 11.7.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	08-May-2023	9.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory **CVE ID : CVE-2023-27953**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1686
N/A	08-May-2023	9.1	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory **CVE ID : CVE-2023-27958**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1687
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://supp	O-APP-MACO-170523/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27946**	ort.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1689
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT21367	O-APP-MACO-170523/1690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to read arbitrary files **CVE ID : CVE-2023-27955**	0, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1691
N/A	08-May-2023	5.5	A logic issue was addressed with	https://support.apple.co	O-APP-MACO-170523/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system **CVE ID : CVE-2023-27962**	m/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
Incorrect Default Permissions	08-May-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information **CVE ID : CVE-2023-28192**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1693
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory **CVE ID : CVE-2023-28200**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670,	O-APP-MACO-170523/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213677	
Affected Version(s): From (including) 12.0 Up to (excluding) 12.6.4					
Out-of-bounds Write	08-May-2023	9.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory **CVE ID : CVE-2023-27953**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1695
N/A	08-May-2023	9.1	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory **CVE ID : CVE-2023-27958**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1696
N/A	08-May-2023	8.8	The issue was addressed with improved bounds checks. This issue is	https://support.apple.com/en-us/HT21367	O-APP-MACO-170523/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27935**	5, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	8.6	This issue was addressed with a new entitlement. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox **CVE ID : CVE-2023-27944**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1698
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://supp	O-APP-MACO-170523/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27936	ort.apple.com/en-us/HT213677	
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1700
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4,	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT21367	O-APP-MACO-170523/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27946**	3, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27949**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1702
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678,	O-APP-MACO-170523/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without prompting the user **CVE ID : CVE-2023-27963**	https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1704
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4,	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-	O-APP-MACO-170523/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper **CVE ID : CVE-2023-27951**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1706
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey	https://support.apple.com/en-us/HT213675, https://supp	O-APP-MACO-170523/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files **CVE ID : CVE-2023-27955**	ort.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-	O-APP-MACO-170523/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213677	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system **CVE ID : CVE-2023-27962**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1709
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences **CVE ID : CVE-2023-28178**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1710
Incorrect Default Permissions	08-May-2023	5.5	A permissions issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://supp	O-APP-MACO-170523/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28192	ort.apple.com/en-us/HT213677	
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory **CVE ID : CVE-2023-28200**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1712
Affected Version(s): From (including) 13.0 Up to (excluding) 13.3					
N/A	08-May-2023	9.8	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A remote user may be able to cause unexpected app termination or arbitrary code execution	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-	O-APP-MACO-170523/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28201	us/HT213676	
Out-of-bounds Write	08-May-2023	9.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory **CVE ID : CVE-2023-27953**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1714
N/A	08-May-2023	9.1	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory **CVE ID : CVE-2023-27958**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1715
N/A	08-May-2023	8.8	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-	O-APP-MACO-170523/1716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11.7.5. A remote user may be able to cause unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27935**	us/HT213670, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	8.6	This issue was addressed with a new entitlement. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to break out of its sandbox **CVE ID : CVE-2023-27944**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1717
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27946**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-May-2023	7.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27949**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1719
Out-of-bounds Write	08-May-2023	7.8	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to cause unexpected system termination or write kernel memory **CVE ID : CVE-2023-27936**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1720
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS	https://support.apple.com/en-us/HT213674, https://supp	O-APP-MACO-170523/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	ort.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27957**	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1722
Out-of-bounds Write	08-May-2023	7.8	A memory corruption issue was addressed with improved state	https://support.apple.com/en-us/HT21367	O-APP-MACO-170523/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27965**	2, https://support.apple.com/en-us/HT213670	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1724
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey	https://support.apple.com/en-us/HT213673, https://support.apple.co	O-APP-MACO-170523/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user **CVE ID : CVE-2023-27963**	m/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.1	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory **CVE ID : CVE-2023-27968**	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1726
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.co	O-APP-MACO-170523/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27933**	m/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-May-2023	6.5	The issue was addressed with improved authentication. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A user in a privileged network position may be able to spoof a VPN server that is configured with EAP-only authentication on a device **CVE ID : CVE-2023-28182**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1729
N/A	08-May-2023	6.3	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to break out of its sandbox **CVE ID : CVE-2023-27966**	https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1730
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-	O-APP-MACO-170523/1731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27956**	us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system **CVE ID : CVE-2023-23533**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1732
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23534**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670	O-APP-MACO-170523/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1734
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to modify protected parts of the file system	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-	O-APP-MACO-170523/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27962	us/HT213677	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-MACO-170523/1736
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://supp	O-APP-MACO-170523/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	ort.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4. An app may be able to modify protected parts of the file system **CVE ID : CVE-2023-23538**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1738
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27942**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.co	O-APP-MACO-170523/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/HT213676, https://support.apple.com/en-us/HT213677, https://support.apple.com/kb/HT213675	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An archive may be able to bypass Gatekeeper **CVE ID : CVE-2023-27951**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1740
N/A	08-May-2023	5.5	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 16.4 and iPadOS 16.4. An app may be able to bypass Privacy preferences **CVE ID : CVE-2023-28178**	https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1742
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to view sensitive information **CVE ID : CVE-2023-28189**	https://support.apple.com/en-us/HT213670, https://support.apple.com/kb/HT213675	O-APP-MACO-170523/1743
Incorrect Default	08-May-2023	5.5	A permissions issue was addressed with improved validation.	https://support.apple.com/en-	O-APP-MACO-170523/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5. An app may be able to read sensitive location information **CVE ID : CVE-2023-28192**	us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	
Improper Input Validation	08-May-2023	5.5	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Big Sur 11.7.5. An app may be able to disclose kernel memory **CVE ID : CVE-2023-28200**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213677	O-APP-MACO-170523/1745
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4. An app may be able to read arbitrary files	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://supp	O-APP-MACO-170523/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27955	ort.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Product: mac_os_x					
Affected Version(s): From (including) 10.0 Up to (excluding) 10.4.8					
N/A	08-May-2023	7.8	This issue was addressed by removing the vulnerable code. This issue is fixed in GarageBand for macOS 10.4.8. An app may be able to gain elevated privileges during the installation of GarageBand **CVE ID : CVE-2023-27960**	https://support.apple.com/en-us/HT213650	O-APP-MAC_-170523/1747
Product: safari					
Affected Version(s): * Up to (excluding) 16.4					
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671,	O-APP-SAFA-170523/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27932	https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
Product: studio_display_firmware					
Affected Version(s): * Up to (excluding) 16.4					
Out-of-bounds Write	08-May-2023	7.8	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Studio Display Firmware Update 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27965**	https://support.apple.com/en-us/HT213672, https://support.apple.com/en-us/HT213670	O-APP-STUD-170523/1749
Product: tvos					
Affected Version(s): * Up to (excluding) 16.4					
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-	O-APP-TVOS-170523/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-TVOS-170523/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-28181**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-TVOS-170523/1752
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27933**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-	O-APP-TVOS-170523/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213677	
Out-of-bounds Read	08-May-2023	6.5	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in tvOS 16.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted Bluetooth packet may result in disclosure of process memory **CVE ID : CVE-2023-23528**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213676	O-APP-TVOS-170523/1754
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://supp	O-APP-TVOS-170523/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-TVOS-170523/1756
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT21367	O-APP-TVOS-170523/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	5, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
Out-of-bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27929**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-TVOS-170523/1758
N/A	08-May-2023	5.5	This issue was addressed by	https://support.apple.co	O-APP-TVOS-170523/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27931**	m/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/kb/HT213604, https://support.apple.com/kb/HT213603	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy **CVE ID : CVE-2023-27932**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-	O-APP-TVOS-170523/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27942**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677, https://support.apple.com/kb/HT213675	O-APP-TVOS-170523/1761
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213674, https://support.apple.co	O-APP-TVOS-170523/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27956**	m/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
Product: watchos					
Affected Version(s): * Up to (excluding) 9.4					
Integer Overflow or Wraparound	08-May-2023	7.8	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. Parsing a maliciously crafted plist may lead to an unexpected app termination or arbitrary code execution **CVE ID : CVE-2023-27937**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-WATC-170523/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676, https://support.apple.com/en-us/HT213677	
Use After Free	08-May-2023	7.8	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27969**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-WATC-170523/1764
N/A	08-May-2023	7.8	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to execute	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://supp	O-APP-WATC-170523/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges **CVE ID : CVE-2023-28181**	ort.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	7.5	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. A shortcut may be able to use sensitive data with certain actions without prompting the user **CVE ID : CVE-2023-27963**	https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-WATC-170523/1766
N/A	08-May-2023	6.7	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT21367	O-APP-WATC-170523/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 16.4. An app with root privileges may be able to execute arbitrary code with kernel privileges **CVE ID : CVE-2023-27933**	0, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-WATC-170523/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676	
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. A user may gain access to protected parts of the file system **CVE ID : CVE-2023-23527**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-WATC-170523/1769
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213675, https://supp	O-APP-WATC-170523/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-23535**	ort.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information **CVE ID : CVE-2023-23537**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-	O-APP-WATC-170523/1771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/HT213676	
Out-of-bounds Read	08-May-2023	5.5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27929**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-WATC-170523/1772
N/A	08-May-2023	5.5	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, watchOS 9.4, iOS 16.4 and iPadOS 16.4. An app may be able to access user-sensitive data **CVE ID : CVE-2023-27931**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://supp	O-APP-WATC-170523/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/kb/HT213604, https://support.apple.com/kb/HT213603	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy **CVE ID : CVE-2023-27932**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-WATC-170523/1774
N/A	08-May-2023	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3, macOS Monterey 12.6.4, watchOS 9.4, tvOS 16.4, iOS 16.4 and iPadOS 16.4. An app may be able to	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://supp	O-APP-WATC-170523/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access user-sensitive data **CVE ID : CVE-2023-27942**	ort.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677, https://support.apple.com/kb/HT213675	
N/A	08-May-2023	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Processing a maliciously crafted image may result in disclosure of process memory **CVE ID : CVE-2023-27956**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	O-APP-WATC-170523/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-May-2023	5.5	Multiple validation issues were addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4, watchOS 9.4, iOS 15.7.4 and iPadOS 15.7.4, iOS 16.4 and iPadOS 16.4. Importing a maliciously crafted calendar invitation may exfiltrate user information **CVE ID : CVE-2023-27961**	https://support.apple.com/en-us/HT213675, https://support.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676, https://support.apple.com/en-us/HT213677	O-APP-WATC-170523/1777
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	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-ARU-ARUB-170523/1778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d 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-2023-22788**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22789**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-ARU-ARUB-170523/1779
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-ARU-ARUB-170523/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22790**		
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-ARU-ARUB-170523/1781
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-ARU-ARUB-170523/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**		
Vendor: Asus					
Product: rt-ac51u_firmware					
Affected Version(s): * Up to (including) 3.0.0.4.380.8591					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-May-2023	5.2	A Cross-site scripting (XSS) vulnerability in the System Log/General Log page of the administrator web UI in ASUS RT-AC51U wireless router firmware version up to and including 3.0.0.4.380.8591 allows remote attackers to inject arbitrary web script or HTML via a malicious network request. **CVE ID : CVE-2023-29772**	N/A	O-ASU-RT-A-170523/1783
Vendor: Axis					
Product: axis_os					
Affected Version(s): From (including) 11.0.89 Up to (excluding) 11.4.52					
Missing Encryption of Sensitive Data	08-May-2023	5.3	AXIS OS 11.0.X - 11.3.x use a static RSA key in legacy LUA-components to protect Axis-specific source code. The	https://www.axis.com/dam/public/07/0a/20/cve-2023-21404-en-	O-AXI-AXIS-170523/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			static RSA key is not used in any other secure communication nor can it be used to compromise the device or any customer data. **CVE ID : CVE-2023-21404**	US-398426.pdf	
Vendor: Cisco					
Product: spa112_firmware					
Affected Version(s): 1.4.1					
Missing Authentication for Critical Function	04-May-2023	9.8	A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW	O-CIS-SPA1-170523/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			full privileges. Cisco has not released firmware updates to address this vulnerability. **CVE ID : CVE-2023-20126**		
Vendor: contiki-ng					
Product: contiki-ng					
Affected Version(s): * Up to (including) 4.8					
NULL Pointer Dereference	08-May-2023	9.8	The Contiki-NG operating system versions 4.8 and prior can be triggered to dereference a NULL pointer in the message handling code for IPv6 router solicitiations. Contiki-NG contains an implementation of IPv6 Neighbor Discovery (ND) in the module `os/net/ipv6/uip-nd6.c`. The ND protocol includes a message type called Router Solicitation (RS), which is used to locate routers and update their address information via the SLLAO (Source Link-Layer Address Option). If the indicated source address changes, a given neighbor entry is set to the STALE state.	https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-x29r-5qjg-75mq	O-CON-CONT-170523/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The message handler does not check for RS messages with an SLLAO that indicates a link-layer address change that a neighbor entry can actually be created for the indicated address. The resulting pointer is used without a check, leading to the dereference of a NULL pointer of type `uip_ds6_nbr_t`. The problem has been patched in the `develop` branch of Contiki-NG, and will be included in the upcoming 4.9 release. As a workaround, users can apply Contiki-NG pull request #2271 to patch the problem directly. **CVE ID : CVE-2023-31129**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
N/A	08-May-2023	6.5	The issue was addressed by removing origin information. This issue is fixed in macOS Ventura 13.3,	https://support.apple.com/en-us/HT213674, https://supp	O-DEB-DEBI-170523/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			watchOS 9.4, tvOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. A website may be able to track sensitive user information **CVE ID : CVE-2023-27954**	ort.apple.com/en-us/HT213673, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678, https://support.apple.com/en-us/HT213676	
N/A	08-May-2023	5.5	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, watchOS 9.4, tvOS 16.4, Safari 16.4, iOS 16.4 and iPadOS 16.4. Processing maliciously crafted web content may bypass Same Origin Policy **CVE ID : CVE-2023-27932**	https://support.apple.com/en-us/HT213674, https://support.apple.com/en-us/HT213670, https://support.apple.com/en-us/HT213671, https://support.apple.com/en-us/HT213678,	O-DEB-DEBI-170523/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT213676	
Affected Version(s): 11.0					
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2023-2461**	N/A	O-DEB-DEBI-170523/1789
Improper Input Validation	03-May-2023	7.1	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2460**	N/A	O-DEB-DEBI-170523/1790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-May-2023	6.5	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2459**	N/A	O-DEB-DEBI-170523/1791
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2462**	N/A	O-DEB-DEBI-170523/1792
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	N/A	O-DEB-DEBI-170523/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2463		
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2464**	N/A	O-DEB-DEBI-170523/1794
N/A	03-May-2023	4.3	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2465**	N/A	O-DEB-DEBI-170523/1795
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page.	N/A	O-DEB-DEBI-170523/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: Low) **CVE ID : CVE-2023-2466**		
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2467**	N/A	O-DEB-DEBI-170523/1797
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2468**	N/A	O-DEB-DEBI-170523/1798
Vendor: Dlink					
Product: dir-868l_firmware					
Affected Version(s): 1.12					
Buffer Copy without	02-May-2023	9.8	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-868L	https://www.dlink.com/en/security-	O-DLI-DIR--170523/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Hardware version A1, firmware version 1.12 is vulnerable to Buffer Overflow. The vulnerability is in scandir.sgi binary. **CVE ID : CVE-2023-29856**	bulletin/, https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10325	
Product: dir-879_firmware					
Affected Version(s): 1.10					
Improper Authentication	01-May-2023	7.5	D-Link DIR-879 v105A1 is vulnerable to Authentication Bypass via phpcgi. **CVE ID : CVE-2023-30061**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--170523/1800
Product: dir-890l_firmware					
Affected Version(s): 1.05					
Improper Authentication	01-May-2023	7.5	D-Link DIR-890L FW1.10 A1 is vulnerable to Authentication bypass. **CVE ID : CVE-2023-30063**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--170523/1801
Vendor: ez-net					
Product: next-7004n_firmware					
Affected Version(s): 3.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-May-2023	6.1	A vulnerability was found in NEXTU NEXT-7004N 3.0.1. It has been classified as problematic. Affected is an unknown function of the file /boafrm/formFilter of the component POST Request	N/A	O-EZ--NEXT-170523/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Handler. The manipulation of the argument url with the input <svg onload=alert(1337)> leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-228012. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2521**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. **CVE ID : CVE-2023-30944**	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77187	O-FED-FEDO-170523/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Divide By Zero	05-May-2023	6.5	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round () function in box.cc, which causes a denial of service. **CVE ID : CVE-2023-29659**	N/A	O-FED-FEDO-170523/1804
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. **CVE ID : CVE-2023-30943**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77718, https://moodle.org/mod/forum/discuss.php?d=446285, https://bugzilla.redhat.com/show_bug.cgi?id=2188605	O-FED-FEDO-170523/1805
Affected Version(s): 37					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/g	O-FED-FEDO-170523/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected application and execute limited SQL commands within the application database. **CVE ID : CVE-2023-30944**	w?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77187	
Divide By Zero	05-May-2023	6.5	A Segmentation fault caused by a floating point exception exists in libheif 1.15.1 using crafted heif images via the heif::Fraction::round() function in box.cc, which causes a denial of service. **CVE ID : CVE-2023-29659**	N/A	O-FED-FEDO-170523/1807
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. **CVE ID : CVE-2023-30943**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77718, https://moodle.org/mod/forum/discuss.php?d=446285, https://bugzilla.redhat.com/show_bug.cgi?id=2188605	O-FED-FEDO-170523/1808
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63	N/A	O-FED-FEDO-170523/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2462**		
Affected Version(s): 38					
Improper Input Validation	07-May-2023	9.8	In Django 3.2 before 3.2.19, 4.x before 4.1.9, and 4.2 before 4.2.1, it was possible to bypass validation when using one form field to upload multiple files. This multiple upload has never been supported by forms.FileField or forms.ImageField (only the last uploaded file was validated). However, Django's "Uploading multiple files" documentation suggested otherwise. **CVE ID : CVE-2023-31047**	https://www.djangoproject.com/weblog/2023/may/03/security-releases/, https://docs.djangoproject.com/en/4.2/releases/security/	O-FED-FEDO-170523/1810
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit	N/A	O-FED-FEDO-170523/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via crafted UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2023-2461**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-May-2023	7.3	The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database. **CVE ID : CVE-2023-30944**	https://moodle.org/mod/forum/discuss.php?d=446286, https://bugzilla.redhat.com/show_bug.cgi?id=2188606, http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77187	O-FED-FEDO-170523/1812
Improper Input Validation	03-May-2023	7.1	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium)	N/A	O-FED-FEDO-170523/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2460		
N/A	03-May-2023	6.5	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2459**	N/A	O-FED-FEDO-170523/1814
Externally Controlled Reference to a Resource in Another Sphere	02-May-2023	5.3	The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system. **CVE ID : CVE-2023-30943**	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-77718, https://moodle.org/mod/forum/discuss.php?d=446285, https://bugzilla.redhat.com/show_bug.cgi?id=2188605	O-FED-FEDO-170523/1815
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the	N/A	O-FED-FEDO-170523/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2463**		
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2464**	N/A	O-FED-FEDO-170523/1817
N/A	03-May-2023	4.3	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2465**	N/A	O-FED-FEDO-170523/1818
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63	N/A	O-FED-FEDO-170523/1819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2466**		
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2467**	N/A	O-FED-FEDO-170523/1820
N/A	03-May-2023	4.3	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2468**	N/A	O-FED-FEDO-170523/1821
Vendor: feiyuxing					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: vec40g_firmware					
Affected Version(s): 3.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-May-2023	7.2	A vulnerability was found in Chengdu VEC40G 3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /send_order.cgi?parameter=access_detect of the component Network Detection. The manipulation of the argument COUNT with the input 3 | netstat -an leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-228013 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2522**	N/A	O-FEI-VEC4-170523/1822
Vendor: fiio					
Product: m6_firmware					
Affected Version(s): 1.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	7.8	A buffer overflow in the component /proc/ftxxxx-debug of FiiO M6 Build Number v1.0.4 allows attackers to escalate privileges to root. **CVE ID : CVE-2023-30257**	N/A	O-FII-M6_F-170523/1823
Vendor: Fortinet					
Product: fortios					
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.16					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via	https://fortiguard.com/psirt/FG-IR-22-475	O-FOR-FORT-170523/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically crafted requests. **CVE ID : CVE-2023-22640**		
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.14					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**	https://fortiguard.com/psirt/FG-IR-22-475	O-FOR-FORT-170523/1825
Affected Version(s): From (including) 6.4.0 Up to (excluding) 6.4.12					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3,	https://fortiguard.com/psirt/FG-IR-22-475	O-FOR-FORT-170523/1826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.11					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1,	https://fortiguard.com/psirt/FG-IR-22-475	O-FOR-FORT-170523/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**		
Affected Version(s): From (including) 7.2.0 Up to (excluding) 7.2.4					
Out-of-bounds Write	03-May-2023	8.8	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows	https://fortiguard.com/psirt/FG-IR-22-475	O-FOR-FORT-170523/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an authenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE ID : CVE-2023-22640**		
Vendor: garo					
Product: wallbox_glb_firmware					
Affected Version(s): * Up to (including) 189					
Incorrect Permission Assignment for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack. **CVE ID : CVE-2023-30399**	N/A	O-GAR-WALL-170523/1829
Product: wallbox_gtb_firmware					
Affected Version(s): * Up to (including) 189					
Incorrect Permission Assignment for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack. **CVE ID : CVE-2023-30399**	N/A	O-GAR-WALL-170523/1830
Product: wallbox_gtc_firmware					
Affected Version(s): * Up to (including) 189					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	04-May-2023	8.1	Insecure permissions in the settings page of GARO Wallbox GLB/GTB/GTC before v189 allows attackers to redirect users to a crafted update package link via a man-in-the-middle attack. **CVE ID : CVE-2023-30399**	N/A	O-GAR-WALL-170523/1831
Vendor: gl-inet					
Product: gl-mt3000_firmware					
Affected Version(s): 4.1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-May-2023	9.8	GL.iNET MT3000 4.1.0 Release 2 is vulnerable to OS Command Injection via /usr/lib/oui-httpd/rpc/logread. **CVE ID : CVE-2023-29778**	N/A	O-GL--GL-M-170523/1832
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	03-May-2023	4.3	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium	N/A	O-GOO-ANDR-170523/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Medium) **CVE ID : CVE-2023-2463**		
N/A	03-May-2023	4.3	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-2467**	N/A	O-GOO-ANDR-170523/1834
Product: chrome_os					
Affected Version(s): -					
Use After Free	03-May-2023	8.8	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium) **CVE ID : CVE-2023-2461**	N/A	O-GOO-CHRO-170523/1835
Vendor: H3C					
Product: gr-1200w_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): minigrw1a0v100r006					
Out-of-bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function set_tftp_upgrad. **CVE ID : CVE-2023-29693**	N/A	O-H3C-GR-1-170523/1836
Out-of-bounds Write	08-May-2023	9.8	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function version_set. **CVE ID : CVE-2023-29696**	N/A	O-H3C-GR-1-170523/1837
Vendor: HP					
Product: arubaos					
Affected Version(s): From (including) 10.3.0.0 Up to (including) 10.3.1.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22780**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PAPI (Aruba's 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-2023-22781**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22782**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22783**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22784**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22785**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1844
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-ARUB-170523/1845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22786**		
Product: instantos					
Affected Version(s): From (including) 6.4.0.0 Up to (including) 6.4.4.8-4.2.4.20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-006.txt	O-HP-INST-170523/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22780**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22781**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22782**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1849
Buffer Copy without Checking	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying	https://www.arubanetworks.com/assets/alert/A	O-HP-INST-170523/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22783**	RUBA-PSA-2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. **CVE ID : CVE-2023-22784**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22785**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1852
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22786**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22788**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1854
Improper Neutralization of Special Elements used in a Command ('Comman	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			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-2023-22789**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22790**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1856
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**		
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1858
Affected Version(s): From (including) 6.5.0.0 Up to (including) 6.5.4.23					
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-006.txt	O-HP-INST-170523/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22780		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22781**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1861
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211).	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22782**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22783**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1863
Buffer Copy without Checking Size of Input	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to	https://ww w.arubanetw orks.com/as sets/alert/A	O-HP-INST-170523/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22784**	RUBA-PSA-2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22785**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22786**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1866
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22788**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22789**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1868
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-006.txt	O-HP-INST-170523/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system. **CVE ID : CVE-2023-22790**		
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1870
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**		
Affected Version(s): From (including) 8.10.0.0 Up to (including) 8.10.0.4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22779**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1872
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted packets destined to the PAPI (Aruba's 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-2023-22780**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22781**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22782**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22783**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22784**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1877
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22785**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-006.txt	O-HP-INST-170523/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22786		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22788**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1880
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22789**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22790**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1882
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1883
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of	https://www.arubanetworks.com/assets/alert/A	O-HP-INST-170523/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**	RUBA-PSA-2023-006.txt	
Affected Version(s): From (including) 8.4.0.0 Up to (excluding) 8.6.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22779**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22780**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1886
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the PAPI (Aruba's 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-2023-22781**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22782**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22783**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22784**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22785**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1891
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22786**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22788**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1893
Improper Neutralization of Special Elements	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba	https://www.arubanetworks.com/assets/alert/A	O-HP-INST-170523/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			InstantOS and ArubaOS 10 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-2023-22789**	RUBA-PSA-2023-006.txt	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22790**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1895
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**		
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1897
Affected Version(s): From (including) 8.6.0.0 Up to (including) 8.6.0.19					
Buffer Copy without Checking	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying	https://www.arubanetworks.com/assets/alert/A	O-HP-INST-170523/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22779**	RUBA-PSA-2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system. **CVE ID : CVE-2023-22780**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22781**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22782**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22783**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1902
Buffer Copy without	08-May-2023	9.8	There are buffer overflow vulnerabilities in	https://www.arubanetworks.com/as	O-HP-INST-170523/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22784**	sets/alert/A RUBA-PSA-2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22785**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22786**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1905
Improper Neutralizat ion of Special Elements used in a Command ('Comman d Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22788**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22789**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1907
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands as a privileged user on the underlying operating system. **CVE ID : CVE-2023-22790**		
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1909
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information can occur are complex and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**		
Affected Version(s): From (including) 8.7.0.0 Up to (including) 8.9.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22779**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1911
Buffer Copy without Checking Size of Input ('Classic	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			ote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-22780**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's 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-2023-006.txt	O-HP-INST-170523/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22781		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22782**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211).	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2023-22783**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22784**	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1916
Buffer Copy without Checking Size of Input	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to	https://ww w.arubanetw orks.com/as sets/alert/A	O-HP-INST-170523/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) 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-2023-22785**	RUBA-PSA-2023-006.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-May-2023	9.8	There are buffer overflow vulnerabilities in multiple underlying services that could lead to unauthenticated rem ote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protoco l) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the	https://ww w.arubanetw orks.com/as sets/alert/A RUBA-PSA-2023-006.txt	O-HP-INST-170523/1918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system. **CVE ID : CVE-2023-22786**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22788**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1919
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-006.txt	O-HP-INST-170523/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22789		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-May-2023	8.8	Multiple authenticated command injection vulnerabilities exist in the Aruba InstantOS and ArubaOS 10 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-2023-22790**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1921
N/A	08-May-2023	7.5	An unauthenticated Denial of Service (DoS) vulnerability exists in a service accessed via the PAPI protocol provided by Aruba InstantOS and ArubaOS 10. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point. **CVE ID : CVE-2023-22787**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-006.txt	O-HP-INST-170523/1922
N/A	08-May-2023	4.8	A vulnerability exists in Aruba InstantOS	https://www.arubanetw	O-HP-INST-170523/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and ArubaOS 10 where an edge-case combination of network configuration, a specific WLAN environment and an attacker already possessing valid user credentials on that WLAN can lead to sensitive information being disclosed via the WLAN. The scenarios in which this disclosure of potentially sensitive information can occur are complex and depend on factors that are beyond the control of the attacker. **CVE ID : CVE-2023-22791**	orks.com/assets/alert/ARUBA-PSA-2023-006.txt	
Product: integrated_lights-out_firmware					
Affected Version(s): 1.05					
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04472en_us	O-HP-INTE-170523/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28092		
Product: proliant_rl300_firmware					
Affected Version(s): 1.12					
N/A	01-May-2023	6.8	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis. **CVE ID : CVE-2023-28092**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04472en_us	O-HP-PROL-170523/1925
Vendor: IBM					
Product: 3948-ved_firmware					
Affected Version(s): From (including) 8.53.0 Up to (including) 8.53.0.63					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	O-IBM-3948-170523/1926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: 3957-vec_firmware					
Affected Version(s): From (including) 8.51.0 Up to (excluding) 8.51.2.12					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	O-IBM-3957-170523/1927
Affected Version(s): From (including) 8.52.100.0 Up to (excluding) 8.52.102.13					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	O-IBM-3957-170523/1928
Product: 3957-ved_firmware					
Affected Version(s): From (including) 8.51.0 Up to (excluding) 8.51.2.12					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700	https://exchange.xforce.i	O-IBM-3957-170523/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	bmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	
Affected Version(s): From (including) 8.52.100.0 Up to (excluding) 8.52.102.13					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	O-IBM-3957-170523/1930
Affected Version(s): From (including) 8.52.200.0 Up to (excluding) 8.52.200.111					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/s	O-IBM-3957-170523/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	upport/pages/node/6980845	
Affected Version(s): From (including) 8.53.0 Up to (excluding) 8.53.0.63					
N/A	04-May-2023	8.8	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320. **CVE ID : CVE-2023-24958**	https://exchange.xforce.ibmcloud.com/vulnerabilities/246320, https://www.ibm.com/support/pages/node/6980845	O-IBM-3957-170523/1932
Product: i					
Affected Version(s): 7.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the	https://exchange.xforce.ibmcloud.com/vulnerabilities/244510, https://www.ibm.com/support/pages/node/6987767	O-IBM-I-170523/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator could exploit the vulnerability to perform additional administrator operations. IBM X-Force ID: 244510. **CVE ID : CVE-2023-23470**		
Affected Version(s): 7.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X-Force ID: 244510. **CVE ID : CVE-2023-23470**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244510, https://www.ibm.com/support/pages/node/6987767	O-IBM-I-170523/1934
Affected Version(s): 7.4					
Improper Neutralization of Special Elements used in an SQL Command	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper	https://exchange.xforce.ibmcloud.com/vulnerabilities/244510, https://www.ibm.com/support/page	O-IBM-I-170523/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X-Force ID: 244510. **CVE ID : CVE-2023-23470**	s/node/6987767	
Affected Version(s): 7.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	7.2	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X-Force ID: 244510. **CVE ID : CVE-2023-23470**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244510, https://www.ibm.com/support/pages/node/6987767	O-IBM-I-170523/1936
Vendor: kaiostech					
Product: kaios					
Affected Version(s): 3.0					
N/A	01-May-2023	5.3	An issue was discovered in KaiOS	N/A	O-KAI-KAIO-170523/1937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.0. The pre-installed Communications application exposes a Web Activity that returns the user's call log without origin or permission checks. An attacker can inject a JavaScript payload that runs in a browser or app without user interaction or consent. This allows an attacker to send the user's call logs to a remote server via XMLHttpRequest or Fetch. **CVE ID : CVE-2023-27108**		
Vendor: Lenovo					
Product: smart_clock_essential_with_alexa_built_in_firmware					
Affected Version(s): * Up to (excluding) 90					
N/A	01-May-2023	8.8	A default password was reported in Lenovo Smart Clock Essential with Alexa Built In that could allow unauthorized device access to an attacker with local network access. **CVE ID : CVE-2023-0896**	https://support.lenovo.com/us/en/product_security/LEN-113714	O-LEN-SMAR-170523/1938
Product: thinkagile_hx1021_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only	https://support.lenovo.com/us/en/pr	O-LEN-THIN-170523/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	oduct_security/LEN-99936	
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1940
Product: thinkagile_hx1320_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1941
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx1321_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1943
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1944
Product: thinkagile_hx1331_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1946
Product: thinkagile_hx1520-r_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1947
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1948
Product: thinkagile_hx1521-r_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1949
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1950
Product: thinkagile_hx2320-e_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1951
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx2321_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1953
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1954
Product: thinkagile_hx2330_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1956
Affected Version(s): 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1957
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx2331_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1959
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1960
Product: thinkagile_hx2720-e_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1961
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_hx3320_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1963
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1964
Product: thinkagile_hx3321_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1965
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1966
Product: thinkagile_hx3330_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1967
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx3331_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1969
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1970
Affected Version(s): * Up to (excluding) 4.71_d8bt48p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0683		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1972
Product: thinkagile_hx3375_firmware					
Affected Version(s): * Up to (excluding) 4.71_d8bt48p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1973
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: thinkagile_hx3376_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1975
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1976
Product: thinkagile_hx3520-g_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1977
Use of Externally-Controlled	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC	https://support.lenovo.com/us/en/product_securi	O-LEN-THIN-170523/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	ty/LEN-99936	
Product: thinkagile_hx3521-g_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1979
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1980
Product: thinkagile_hx3720_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_securi	O-LEN-THIN-170523/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**	ty/LEN-99936	
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1982
Product: thinkagile_hx3721_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1983
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx5520-c_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1985
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1986
Product: thinkagile_hx5520_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1987
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_hx5521-c_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1989
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1990
Product: thinkagile_hx5521_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1991
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1992
Product: thinkagile_hx5530_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1993
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx5531_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1995
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1996
Product: thinkagile_hx7520_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1998
Product: thinkagile_hx7521_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/1999
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_hx7530_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2001
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2002
Product: thinkagile_hx7531_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2003
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Affected Version(s): * Up to (excluding) 2.75_psi348s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2005
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2006
Product: thinkagile_hx7820_firmware					
Affected Version(s): * Up to (excluding) 2.75_psi348s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only	https://support.lenovo.com/us/en/pr	O-LEN-THIN-170523/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	oduct_security/LEN-99936	
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2008
Product: thinkagile_hx7821_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2009
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_hx_enclosure_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2011
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2012
Product: thinkagile_mx1020_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2014
Product: thinkagile_mx1021_on_se350_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2015
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2016
Product: thinkagile_mx3330-f_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2017
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2018
Product: thinkagile_mx3330-h_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2019
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_mx3331-f_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2021
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2022
Product: thinkagile_mx3331-h_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2024
Product: thinkagile_mx3530-h_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2025
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_mx3530_f_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2027
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2028
Product: thinkagile_mx3531-f_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2029
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_mx3531_h_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2031
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2032
Product: thinkagile_vx1320_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2033
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2034
Product: thinkagile_vx2320_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2035
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_vx2330_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2037
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2038
Product: thinkagile_vx3320_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2040
Product: thinkagile_vx3330_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2041
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_vx3331_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2043
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2044
Product: thinkagile_vx3520-g_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2045
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_vx3530-g_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2047
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2048
Product: thinkagile_vx3720_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2049
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2050
Product: thinkagile_vx5520_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2051
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_vx5530_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2053
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2054
Product: thinkagile_vx7320_n_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2056
Product: thinkagile_vx7330_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2057
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkagile_vx7520_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2059
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2060
Product: thinkagile_vx7520_n_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2061
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinkagile_vx7530_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2063
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2064
Product: thinkagile_vx7531_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2065
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2066
Product: thinkagile_vx7820_firmware					
Affected Version(s): * Up to (excluding) 2.75_psi348s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2067
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinkagile_vx_1se_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2069
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2070
Product: thinkagile_vx_2u4n_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2072
Product: thinkagile_vx_4u_firmware					
Affected Version(s): * Up to (excluding) 2.75_psi348s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2073
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinkedge_se450_firmware					
Affected Version(s): * Up to (excluding) 1.60_usx324o					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2075
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2076
Product: thinkstation_p920_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2077
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sd530_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2079
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2080
Product: thinksystem_sd630_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2081
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2082
Product: thinksystem_sd650-n_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2083
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sd650_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2085
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2086
Product: thinksystem_sd650_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2088
Product: thinksystem_se350_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2089
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sn550_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2091
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2092
Product: thinksystem_sn550_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2093
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sn850_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2095
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2096
Product: thinksystem_sr150_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2097
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2098
Product: thinksystem_sr158_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2099
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sr250_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2101
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2102
Product: thinksystem_sr250_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2104
Product: thinksystem_sr258_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2105
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sr258_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2107
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2108
Product: thinksystem_sr530_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2109
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sr550_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2111
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2112
Product: thinksystem_sr570_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2113
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2114
Product: thinksystem_sr590_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2115
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sr630_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2117
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2118
Product: thinksystem_sr630_v2_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2120
Product: thinksystem_sr645_firmware					
Affected Version(s): * Up to (excluding) 4.71_d8bt48p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2121
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sr645_v3_firmware					
Affected Version(s): * Up to (excluding) 4.71_d8bt48p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2123
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2124
Product: thinksystem_sr650_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2125
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sr650_v2_firmware					
Affected Version(s): * Up to (excluding) 2.93_afbt30p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2127
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2128
Product: thinksystem_sr665_firmware					
Affected Version(s): * Up to (excluding) 4.71_d8bt48p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2129
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2130
Product: thinksystem_sr665_v3_firmware					
Affected Version(s): * Up to (excluding) 4.71_d8bt48p					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2131
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_sr670_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2133
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2134
Product: thinksystem_sr670_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2136
Product: thinksystem_sr850p_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2137
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_sr850_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2139
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2140
Product: thinksystem_sr850_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2141
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_sr860_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2143
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2144
Product: thinksystem_sr860_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2145
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2146
Product: thinksystem_sr950_firmware					
Affected Version(s): * Up to (excluding) 2.75_psi348s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2147
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**		
Product: thinksystem_st250_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2149
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2150
Product: thinksystem_st250_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through a specifically crafted API call. **CVE ID : CVE-2023-0683**		
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2152
Product: thinksystem_st258_firmware					
Affected Version(s): * Up to (excluding) 3.72_tei388s					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2153
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25492		
Product: thinksystem_st258_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2155
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2156
Product: thinksystem_st550_firmware					
Affected Version(s): * Up to (excluding) 8.88_cdi3a4a					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2157
Use of Externally-	01-May-2023	8.8	A valid, authenticated user	https://support.lenovo.co	O-LEN-THIN-170523/2158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	m/us/en/product_security/LEN-99936	
Product: thinksystem_st650_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2159
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2160
Product: thinksystem_st658_v2_firmware					
Affected Version(s): * Up to (excluding) 2.60_tgbt42h					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-May-2023	8.8	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call. **CVE ID : CVE-2023-0683**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2161
Use of Externally-Controlled Format String	01-May-2023	8.8	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API. **CVE ID : CVE-2023-25492**	https://support.lenovo.com/us/en/product_security/LEN-99936	O-LEN-THIN-170523/2162
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 6.1.11					
Use After Free	05-May-2023	6.7	An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netrom.c, there is a use-after-free because accept is also allowed for a successfully connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have	https://github.com/torvalds/linux/commit/611792920925fb088ddccbe2783c7f92fdfb6b64	O-LIN-LINU-170523/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netrom routing configured or the attacker must have the CAP_NET_ADMIN capability. **CVE ID : CVE-2023-32269**		
Affected Version(s): * Up to (including) 5.19					
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. **CVE ID : CVE-2023-2513**	https://github.com/torvalds/linux/commit/67d7d8ad99be	O-LIN-LINU-170523/2164
Affected Version(s): * Up to (including) 6.3.1					
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.	https://github.com/torvalds/linux/commit/c1592a89942e9678f7d9c8030efa777c0d57edab, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c1592a89942e9678f7d9c	O-LIN-LINU-170523/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32233	8030efa777c0d57edab	
Affected Version(s): 6.1					
Use After Free	01-May-2023	7.8	A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Both io_install_fixed_file and its callers call fput in a file in case of an error, causing a reference underflow which leads to a use-after-free vulnerability. We recommend upgrading past commit 9d94c04c0db024922e886c9fd429659f22f48ea4. **CVE ID : CVE-2023-2236**	https://kernel.dance/9d94c04c0db024922e886c9fd429659f22f48ea4, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9d94c04c0db024922e886c9fd429659f22f48ea4	O-LIN-LINU-170523/2166
Affected Version(s): 6.3					
Use After Free	01-May-2023	7.8	A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation.	https://kernel.dance/fd0815f632c24878e325821943edccc7fde947a2, https://git.kernel.org/pub/scm/linux	O-LIN-LINU-170523/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The perf_group_detach function did not check the event's siblings' attach_state before calling add_event_to_groups (), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a dangling pointer causing a use-after-free vulnerability. We recommend upgrading past commit fd0815f632c24878e325821943edccc7fde947a2. **CVE ID : CVE-2023-2235**	/kernel/git/torvalds/linux.git/commit/?id=fd0815f632c24878e325821943edccc7fde947a2	
Affected Version(s): From (including) 5.13 Up to (excluding) 6.3					
Use After Free	01-May-2023	7.8	A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation. The perf_group_detach	https://kernel.dance/fd0815f632c24878e325821943edccc7fde947a2, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit	O-LIN-LINU-170523/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function did not check the event's siblings' attach_state before calling add_event_to_groups (), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a dangling pointer causing a use-after-free vulnerability. We recommend upgrading past commit fd0815f632c24878e325821943edccc7fde947a2. **CVE ID : CVE-2023-2235**	/?id=fd0815f632c24878e325821943edccc7fde947a2	
Affected Version(s): From (including) 5.19 Up to (excluding) 6.1					
Use After Free	01-May-2023	7.8	A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Both io_install_fixed_file and its callers call fput in a file in case of an error, causing a reference	https://kernel.dance/9d94c04c0db024922e886c9fd429659f22f48ea4, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9d94c04c0db02492	O-LIN-LINU-170523/2169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underflow which leads to a use-after-free vulnerability. We recommend upgrading past commit 9d94c04c0db024922e886c9fd429659f22f48ea4. **CVE ID : CVE-2023-2236**	2e886c9fd429659f22f48ea4	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-May-2023	9.8	CLTPHP <=6.0 is vulnerable to Improper Input Validation. **CVE ID : CVE-2023-30268**	N/A	O-MIC-WIND-170523/2170
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	03-May-2023	5.9	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://my.f5.com/manage/s/article/K000132522	O-MIC-WIND-170523/2171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22372		
Improper Certificate Validation	03-May-2023	5.9	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2023-24461**	https://my.f5.com/manage/s/article/K000132539	O-MIC-WIND-170523/2172
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.19926					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2173
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2175
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2176
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2177
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2178
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2179
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2181
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2182
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2183
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2184
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2185
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2186
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24945**	ability/CVE-2023-24945	
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2188
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.5921					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2189
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2190
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2191
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP)	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	ability/CVE-2023-28283	
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2193
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2194
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2195
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2196
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2197
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29325	ability/CVE-2023-29325	
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2199
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2200
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2201
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2202
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2203
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2205
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.4377					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2206
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2207
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2208
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28283		
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2210
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24949**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24949	O-MIC-WIND-170523/2211
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2212
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2213
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2214
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2216
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2217
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2218
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2219
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2220
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2221
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24900**	ability/CVE-2023-24900	
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2223
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2224
Product: windows_10_20h2					
Affected Version(s): * Up to (excluding) 10.0.19042.2965					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2225
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2226
Concurrent Execution using Shared Resource with Improper Synchroniz	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			**CVE ID : CVE-2023-24903**		
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2228
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2023-24905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24905	O-MIC-WIND-170523/2229
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2230
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24949**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24949	O-MIC-WIND-170523/2231
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2232
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24939	ability/CVE-2023-24939	
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2234
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2235
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2236
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2237
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2238
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2239
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information	https://msrc.microsoft.co	O-MIC-WIND-170523/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24944**	m/update-guide/vulnerability/CVE-2023-24944	
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2241
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2242
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2243
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2244
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.2965					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2246
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2247
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2248
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2023-24905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24905	O-MIC-WIND-170523/2249
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2250
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24949	guide/vulnerability/CVE-2023-24949	
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2252
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2253
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2254
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2255
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2256
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2258
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2259
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2260
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2261
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2262
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2263
N/A	09-May-2023	5.5	Windows Driver Revocation List	https://msrc.microsoft.co	O-MIC-WIND-170523/2264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	m/update-guide/vulnerability/CVE-2023-28251	
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.2965					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2265
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2266
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2267
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2023-24905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24905	O-MIC-WIND-170523/2269
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2270
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24949**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24949	O-MIC-WIND-170523/2271
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2272
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2273
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2274
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service Vulnerability **CVE ID : CVE-2023-24942**	ability/CVE-2023-24942	
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2276
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2277
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2278
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2279
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2280
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2282
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2283
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2284
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.2965					
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2285
Affected Version(s): * Up to (excluding) 10.0.22000.1702					
Concurrent Execution using Shared Resource with Improper Synchronization	09-May-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24899	O-MIC-WIND-170523/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
Affected Version(s): * Up to (excluding) 10.0.22000.1936					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2287
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2288
N/A	09-May-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24902**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902	O-MIC-WIND-170523/2289
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2023-24905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24905	O-MIC-WIND-170523/2290
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2291
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24949	guide/vulnerability/CVE-2023-24949	
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2293
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2294
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2295
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2296
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2297
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2299
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2300
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2301
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2302
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2303
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2304
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22000.1702					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2305
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2306
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2307
N/A	09-May-2023	7.8	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24902**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902	O-MIC-WIND-170523/2308
N/A	09-May-2023	7.8	Remote Desktop Client Remote Code Execution Vulnerability **CVE ID : CVE-2023-24905**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24905	O-MIC-WIND-170523/2309
N/A	09-May-2023	7.8	Windows Backup Service Elevation of	https://msrc.microsoft.co	O-MIC-WIND-170523/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-24946**	m/update-guide/vulnerability/CVE-2023-24946	
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24949**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24949	O-MIC-WIND-170523/2311
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2312
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2313
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2314
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2315
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29325	ability/CVE-2023-29325	
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2317
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24899	O-MIC-WIND-170523/2318
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2319
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2320
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2321
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24900**	ability/CVE-2023-24900	
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2323
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2324
Product: windows_server_2008					
Affected Version(s): -					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2325
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2326
N/A	09-May-2023	8.1	Windows Lightweight Directory Access	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	guide/vulnerability/CVE-2023-28283	
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2328
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2329
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2330
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2331
N/A	09-May-2023	7.1	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24904	O-MIC-WIND-170523/2332
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24932	ability/CVE-2023-24932	
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2334
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2335
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2336
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2337
Affected Version(s): r2					
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2338
Concurrent Execution using Shared	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Execution Vulnerability **CVE ID : CVE-2023-24903**	ability/CVE-2023-24903	
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2340
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2341
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2342
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2343
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2345
N/A	09-May-2023	7.1	Windows Installer Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24904**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24904	O-MIC-WIND-170523/2346
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2347
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2348
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2349
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2350
N/A	09-May-2023	5.5	Windows Driver Revocation List	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	guide/vulnerability/CVE-2023-28251	
Product: windows_server_2012					
Affected Version(s): -					
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2023-24941**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941	O-MIC-WIND-170523/2352
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2353
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2354
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2356
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2357
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2358
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2359
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2360
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2361
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-24948**	ability/CVE-2023-24948	
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2363
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2364
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2365
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2366
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2367
Affected Version(s): r2					
N/A	09-May-2023	9.8	Windows Network File System Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-24941**	guide/vulnerability/CVE-2023-24941	
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2369
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2370
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2371
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2372
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24939	guide/vulnerability/CVE-2023-24939	
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2374
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2375
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2376
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2377
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2378
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2380
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2381
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2382
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2383
Product: windows_server_2016					
Affected Version(s): -					
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2023-24941**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941	O-MIC-WIND-170523/2384
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24943		
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2386
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2387
N/A	09-May-2023	8.1	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28283	O-MIC-WIND-170523/2388
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2389
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2391
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2392
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2393
N/A	09-May-2023	7.5	Windows OLE Remote Code Execution Vulnerability **CVE ID : CVE-2023-29325**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325	O-MIC-WIND-170523/2394
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2395
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2396
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24932	ability/CVE-2023-24932	
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2398
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24900	O-MIC-WIND-170523/2399
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2400
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2401
Product: windows_server_2019					
Affected Version(s): -					
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2023-24941**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941	O-MIC-WIND-170523/2402
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24943**	ability/CVE-2023-24943	
N/A	09-May-2023	8.8	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24947**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24947	O-MIC-WIND-170523/2404
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2405
N/A	09-May-2023	7.8	Windows Backup Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24946**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24946	O-MIC-WIND-170523/2406
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24949**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24949	O-MIC-WIND-170523/2407
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2409
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2410
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2411
N/A	09-May-2023	7.4	Windows Bluetooth Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24948**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948	O-MIC-WIND-170523/2412
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2413
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2414
N/A	09-May-2023	5.9	Windows NTLM Security Support Provider Information	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24900**	ability/CVE-2023-24900	
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2416
Product: windows_server_2022					
Affected Version(s): -					
N/A	09-May-2023	9.8	Windows Network File System Remote Code Execution Vulnerability **CVE ID : CVE-2023-24941**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941	O-MIC-WIND-170523/2417
N/A	09-May-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24943**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24943	O-MIC-WIND-170523/2418
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-24903**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24903	O-MIC-WIND-170523/2419
N/A	09-May-2023	8.1	Windows Lightweight Directory Access	https://msrc.microsoft.com/update-	O-MIC-WIND-170523/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (LDAP) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28283**	guide/vulnerability/CVE-2023-28283	
N/A	09-May-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24949**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24949	O-MIC-WIND-170523/2421
N/A	09-May-2023	7.5	Windows NFS Portmapper Information Disclosure Vulnerability **CVE ID : CVE-2023-24901**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24901	O-MIC-WIND-170523/2422
N/A	09-May-2023	7.5	Server for NFS Denial of Service Vulnerability **CVE ID : CVE-2023-24939**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24939	O-MIC-WIND-170523/2423
N/A	09-May-2023	7.5	Windows Pragmatic General Multicast (PGM) Denial of Service Vulnerability **CVE ID : CVE-2023-24940**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24940	O-MIC-WIND-170523/2424
N/A	09-May-2023	7.5	Remote Procedure Call Runtime Denial of Service Vulnerability **CVE ID : CVE-2023-24942**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24942	O-MIC-WIND-170523/2425
N/A	09-May-2023	7.5	Windows OLE Remote Code	https://msrc.microsoft.com/update-guide/vulner	O-MIC-WIND-170523/2426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-29325**	ability/CVE-2023-29325	
N/A	09-May-2023	7.5	Microsoft Word Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29335	O-MIC-WIND-170523/2427
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-May-2023	7	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24899**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24899	O-MIC-WIND-170523/2428
N/A	09-May-2023	6.7	Secure Boot Security Feature Bypass Vulnerability **CVE ID : CVE-2023-24932**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	O-MIC-WIND-170523/2429
N/A	09-May-2023	6.5	Windows Bluetooth Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24944**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24944	O-MIC-WIND-170523/2430
N/A	09-May-2023	6.5	Windows MSHTML Platform Security Feature Bypass Vulnerability **CVE ID : CVE-2023-29324**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29324	O-MIC-WIND-170523/2431
N/A	09-May-2023	5.9	Windows NTLM Security Support	https://msrc.microsoft.co	O-MIC-WIND-170523/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Provider Information Disclosure Vulnerability **CVE ID : CVE-2023-24900**	m/update-guide/vulnerability/CVE-2023-24900	
N/A	09-May-2023	5.5	Windows iSCSI Target Service Information Disclosure Vulnerability **CVE ID : CVE-2023-24945**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24945	O-MIC-WIND-170523/2433
N/A	09-May-2023	5.5	Windows Driver Revocation List Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28251**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28251	O-MIC-WIND-170523/2434
Affected Version(s): * Up to (excluding) 10.0.20348.1724					
N/A	09-May-2023	7.5	Windows SMB Denial of Service Vulnerability **CVE ID : CVE-2023-24898**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24898	O-MIC-WIND-170523/2435
Vendor: milesight					
Product: ncr\/camera_firmware					
Affected Version(s): 71.8.0.6-r5					
N/A	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 discloses sensitive information through an unspecified request. **CVE ID : CVE-2023-24505**	N/A	O-MIL-NCR\-170523/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	08-May-2023	7.5	Milesight NCR/camera version 71.8.0.6-r5 exposes credentials through an unspecified request. **CVE ID : CVE-2023-24506**	N/A	O-MIL-NCR\-170523/2437
Vendor: mitrastar					
Product: gpt-2741gnac-n2_firmware					
Affected Version(s): br_g5.9_1.11\\(wvk.0\\)b32					
N/A	05-May-2023	8.8	MitraStar GPT-2741GNAC-N2 with firmware BR_g5.9_1.11(WVK.0)b32 was discovered to contain a remote code execution (RCE) vulnerability in the ping function. **CVE ID : CVE-2023-30065**	N/A	O-MIT-GPT--170523/2438
Vendor: Qualcomm					
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-315_-170523/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: 8905_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8905-170523/2440
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8905-170523/2441
Product: 8909_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8909-170523/2442
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8909-170523/2443
Product: 8917_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8917-170523/2444
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8917-170523/2445
Product: 8952_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8952-170523/2446
Product: 8953pro_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8953-170523/2447
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-8953-170523/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: 8953_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8953-170523/2449
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8953-170523/2450
Product: 8956_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8956-170523/2451
Product: 8976pro_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-8976-170523/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: 8976_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8976-170523/2453
Product: 8998_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8998-170523/2454
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-8998-170523/2455
Product: 9206_lte_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-9206-170523/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: apq5053-aa_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ5-170523/2457
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ5-170523/2458
Product: apq8017_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2459
Product: apq8052_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2460
Product: apq8053-aa_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2461
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2462
Product: apq8053-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2463
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2464
Product: apq8053-lite_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-APQ8-170523/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2466
Product: apq8056_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2467
Product: apq8064au_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-APQ8-170523/2468
Product: apq8076_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-APQ8-170523/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: aqt1000_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-AQT1-170523/2470
Product: ar8031_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-AR80-170523/2471
Product: ar8035_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-AR80-170523/2472
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-C-V2-170523/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: csra6620_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-CSRA-170523/2474
Product: csra6640_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-CSRA-170523/2475
Product: csrb31024_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-CSRB-170523/2476
Product: flight_rb5_5g_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-FLIG-170523/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-FLIG-170523/2478
Product: home_hub_100_platform_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-HOME-170523/2479
Product: mdm9250_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MDM9-170523/2480
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MDM9-170523/2481
Product: mdm9628_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MDM9-170523/2482
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MDM9-170523/2483
Product: mdm9650_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MDM9-170523/2484
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MDM9-170523/2485
Product: msm8108_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-MSM8-170523/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2487
Product: msm8209_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2488
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2489
Product: msm8608_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2491
Product: msm8909w_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2492
Product: msm8996au_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-MSM8-170523/2493
Product: qam8295p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QAM8-170523/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QAM8-170523/2495
Product: qca-4020-0-217msp_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA--170523/2496
Product: qca-4020-1-217msp_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA--170523/2497
Product: qca-4024-0-68cmqfn_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA--170523/2498
Product: qca-4024-1-68cmqfn_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA--170523/2499
Product: qca6174a_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2500
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2501
Product: qca6174_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2502
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-170523/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: qca6310_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2504
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2505
Product: qca6320_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2506
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2507
Product: qca6335_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2508
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2509
Product: qca6390_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2510
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2511
Product: qca6391_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-QCA6-170523/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2513
Product: qca6420_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2514
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2515
Product: qca6421_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2517
Product: qca6426_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2518
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2519
Product: qca6430_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2520
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-170523/2521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: qca6431_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2522
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2523
Product: qca6436_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2524
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2525
Product: qca6564au_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2526
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2527
Product: qca6564a_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2528
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2529
Product: qca6564_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-QCA6-170523/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2531
Product: qca6574au_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2532
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2533
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2534
Product: qca6574a_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2535
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2536
Product: qca6574_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2537
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2538
Product: qca6584au_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-170523/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Product: qca6595au_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2540
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2541
Product: qca6595_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2542
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2543
Product: qca6696_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2544
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2545
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2546
Product: qca6698aq_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA6-170523/2547
Product: qca8081_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/compa	O-QUA-QCA8-170523/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	ny/product-security/bulletins/may-2023-bulletin	
Product: qca8337_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA8-170523/2549
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA8-170523/2550
Product: qca9367_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA9-170523/2551
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA9-170523/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9377_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA9-170523/2553
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA9-170523/2554
Product: qca9379_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA9-170523/2555
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCA9-170523/2556
Product: qcm2290_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCM2-170523/2557
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCM2-170523/2558
Product: qcm4290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCM4-170523/2559
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCM4-170523/2560
Product: qcm6125_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCM6-170523/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCM6-170523/2562
Product: qcm6490_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCM6-170523/2563
Product: qcn6024_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN6-170523/2564
Product: qcn9011_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCN9-170523/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN9-170523/2566
Product: qcn9012_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN9-170523/2567
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN9-170523/2568
Product: qcn9024_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN9-170523/2569
Product: qcn9074_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN9-170523/2570
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCN9-170523/2571
Product: qcs2290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS2-170523/2572
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS2-170523/2573
Product: qcs400_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCS4-170523/2574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Product: qcs410_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS4-170523/2575
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS4-170523/2576
Product: qcs4290_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS4-170523/2577
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS4-170523/2578
Product: qcs605_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS6-170523/2579
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS6-170523/2580
Product: qcs610_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS6-170523/2581
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS6-170523/2582
Product: qcs6125_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-QCS6-170523/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS6-170523/2584
Product: qcs6490_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS6-170523/2585
Product: qcs8155_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS8-170523/2586
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS8-170523/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcs8250_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS8-170523/2588
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QCS8-170523/2589
Product: qm215_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QM21-170523/2590
Product: qrb5165m_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QRB5-170523/2591
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	O-QUA-QRB5-170523/2592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: qrb5165n_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QRB5-170523/2593
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QRB5-170523/2594
Product: qrb5165_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QRB5-170523/2595
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QRB5-170523/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: qsm8250_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QSM8-170523/2597
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-QSM8-170523/2598
Product: sa4150p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA41-170523/2599
Product: sa4155p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA41-170523/2600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa6145p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2601
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2602
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2603
Product: sa6150p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2604
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA61-170523/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2606
Product: sa6155p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2607
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2608
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2609
Product: sa6155_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2610
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA61-170523/2611
Product: sa8145p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2612
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2613
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA81-170523/2614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: sa8150p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2615
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2616
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2617
Product: sa8155p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2619
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2620
Product: sa8155_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2621
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2622
Product: sa8195p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system	https://www.qualcomm.com/company/product-security/bull	O-QUA-SA81-170523/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges via physical address. **CVE ID : CVE-2023-21642**	etins/may-2023-bulletin	
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2624
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA81-170523/2625
Product: sa8295p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA82-170523/2626
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA82-170523/2627
Product: sa8540p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA85-170523/2628
Product: sa9000p_firmware					
Affected Version(s): -					
N/A	02-May-2023	7.8	Memory corruption in HAB Memory management due to broad system privileges via physical address. **CVE ID : CVE-2023-21642**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SA90-170523/2629
Product: sd626_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD62-170523/2630
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD62-170523/2631
Product: sd660_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD66-170523/2632
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD66-170523/2633
Product: sd670_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD67-170523/2634
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD67-170523/2635
Product: sd675_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD67-170523/2636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD67-170523/2637
Product: sd730_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD73-170523/2638
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD73-170523/2639
Product: sd835_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD83-170523/2640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD83-170523/2641
Product: sd855_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD85-170523/2642
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD85-170523/2643
Product: sd865_5g_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD86-170523/2644
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD86-170523/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: sd888_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD88-170523/2646
Product: sda\/sdm845_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDA\-170523/2647
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDA\-170523/2648
Product: sdm429w_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDM4-170523/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM4-170523/2650
Product: sdm429_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM4-170523/2651
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM4-170523/2652
Product: sdm439_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM4-170523/2653
Missing Release of Memory	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer	https://www.qualcomm.com/compa	O-QUA-SDM4-170523/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			allocated through the graphics pool. **CVE ID : CVE-2023-21666**	ny/product-security/bulletins/may-2023-bulletin	
Product: sdm450_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM4-170523/2655
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM4-170523/2656
Product: sdm660_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM6-170523/2657
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM6-170523/2658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sdm670_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM6-170523/2659
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM6-170523/2660
Product: sdm710_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM7-170523/2661
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM7-170523/2662
Product: sdm845_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM8-170523/2663
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDM8-170523/2664
Product: sdx20m_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDX2-170523/2665
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDX2-170523/2666
Product: sdx55_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDX5-170523/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SDX5-170523/2668
Product: sd_675_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD_6-170523/2669
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SD_6-170523/2670
Product: sm4125_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM41-170523/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM41-170523/2672
Product: sm4250-aa_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM42-170523/2673
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM42-170523/2674
Product: sm4350-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM43-170523/2675
Product: sm4350_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM43-170523/2676
Product: sm4375_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM43-170523/2677
Product: sm6115_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2678
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2679
Product: sm6125_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2680
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2681
Product: sm6150-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2682
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2683
Product: sm6150_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM61-170523/2684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM61-170523/2685
Product: sm6225-ad_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2686
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2687
Product: sm6225_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2689
Product: sm6250p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2690
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2691
Product: sm6250_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM62-170523/2692
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM62-170523/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: sm6350_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM63-170523/2694
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM63-170523/2695
Product: sm6375_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM63-170523/2696
Product: sm7125_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SM71-170523/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM71-170523/2698
Product: sm7150-aa_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM71-170523/2699
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM71-170523/2700
Product: sm7150-ab_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM71-170523/2701
Missing Release of Memory	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer	https://www.qualcomm.com/compa	O-QUA-SM71-170523/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			allocated through the graphics pool. **CVE ID : CVE-2023-21666**	ny/product-security/bulletins/may-2023-bulletin	
Product: sm7150-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM71-170523/2703
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM71-170523/2704
Product: sm7225_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2705
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm7250-aa_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2707
Product: sm7250-ab_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2708
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2709
Product: sm7250-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2710
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	O-QUA-SM72-170523/2711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: sm7250p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2712
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM72-170523/2713
Product: sm7315_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM73-170523/2714
Product: sm7325-ae_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-SM73-170523/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	security/bulletins/may-2023-bulletin	
Product: sm7325-af_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM73-170523/2716
Product: sm7325p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM73-170523/2717
Product: sm7325_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM73-170523/2718
Product: sm7350-ab_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-SM73-170523/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Product: sm8150-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM81-170523/2720
Product: sm8150_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM81-170523/2721
Product: sm8250-ab_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM82-170523/2722
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SM82-170523/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21666	2023-bulletin	
Product: sm8250-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM82-170523/2724
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM82-170523/2725
Product: sm8250_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM82-170523/2726
Product: sm8350-ac_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM83-170523/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm8350_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SM83-170523/2728
Product: snapdragon_1200_wearable_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2729
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2730
Product: snapdragon_208_processor_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2731
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	O-QUA-SNAP-170523/2732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: snapdragon_630_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2733
Product: snapdragon_632_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2734
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2735
Product: snapdragon_636_mobile_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-SNAP-170523/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	security/bulletins/may-2023-bulletin	
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2737
Product: snapdragon_820_automotive_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2738
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2739
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SNAP-170523/2740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2741
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2742
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2743
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2744
Product: snapdragon_wear_2100_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2745
Product: snapdragon_wear_2500_platform_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2746
Product: snapdragon_wear_3100_platform_firmware					
Affected Version(s): -					
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2747
Product: snapdragon_wear_4100\+_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2748
Missing Release of	02-May-2023	7.8	Memory Corruption in Graphics while	https://www.qualcomm	O-QUA-SNAP-170523/2749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	.com/company/product-security/bulletins/may-2023-bulletin	
Product: snapdragon_x12_lte_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2750
Product: snapdragon_x20_lte_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2751
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2752
Product: snapdragon_x24_lte_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-SNAP-170523/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21665	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2754
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2755
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2756
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2758
Product: snapdragon_x5_lte_modem_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2759
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2760
Product: snapdragon_x65_5g_modem-rf_system_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2761
Product: snapdragon_xr1_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2762
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2763
Product: snapdragon_xr2\+_gen_1_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2764
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2765
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-SNAP-170523/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SNAP-170523/2767
Product: ssm7250-aa_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SSM7-170523/2768
Product: sw5100p_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SW51-170523/2769
Product: sw5100_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SW51-170523/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2023-bulletin	
Product: sxr1120_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SXR1-170523/2771
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SXR1-170523/2772
Product: sxr2130_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SXR2-170523/2773
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-SXR2-170523/2774
Product: wcd9326_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2775
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2776
Product: wcd9330_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2777
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2778
Product: wcd9335_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-170523/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				etins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2780
Product: wcd9340_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2781
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2782
Product: wcd9341_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2784
Product: wcd9370_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2785
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2786
Product: wcd9371_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2787
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-170523/2788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: wcd9375_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2789
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2790
Product: wcd9380_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2791
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2792
Product: wcd9385_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2793
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCD9-170523/2794
Product: wcn3610_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2795
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2796
Product: wcn3615_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-WCN3-170523/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2798
Product: wcn3620_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2799
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2800
Product: wcn3660b_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2802
Product: wcn3660_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2803
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2804
Product: wcn3680b_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2805
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-170523/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: wcn3680_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2807
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2808
Product: wcn3910_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2809
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2810
Product: wcn3950_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2811
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2812
Product: wcn3980_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2813
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2814
Product: wcn3988_firmware					
Affected Version(s): -					
Incorrect Type	02-May-2023	7.8	Memory corruption in Graphics while importing a file.	https://www.qualcomm.com/company/product-	O-QUA-WCN3-170523/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			**CVE ID : CVE-2023-21665**	security/bulletins/may-2023-bulletin	
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2816
Product: wcn3990_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2817
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2818
Product: wcn3998_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2820
Product: wcn3999_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2821
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN3-170523/2822
Product: wcn6740_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN6-170523/2823
Product: wcn6750_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN6-170523/2824
Product: wcn685x-1_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN6-170523/2825
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN6-170523/2826
Product: wcn685x-5_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WCN6-170523/2827
Missing Release of Memory after	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN6-170523/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Effective Lifetime			**CVE ID : CVE-2023-21666**	etins/may-2023-bulletin	
Product: wsa8810_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2829
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2830
Product: wsa8815_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2831
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2832
Product: wsa8830_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2833
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2834
Product: wsa8835_firmware					
Affected Version(s): -					
Incorrect Type Conversion or Cast	02-May-2023	7.8	Memory corruption in Graphics while importing a file. **CVE ID : CVE-2023-21665**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2835
Missing Release of Memory after Effective Lifetime	02-May-2023	7.8	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool. **CVE ID : CVE-2023-21666**	https://www.qualcomm.com/company/product-security/bulletins/may-2023-bulletin	O-QUA-WSA8-170523/2836
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 6.0					
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was	https://github.com/torval	O-RED-ENTE-170523/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. **CVE ID : CVE-2023-2513**	ds/linux/commit/67d7d8ad99be	
Affected Version(s): 7.0					
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled. **CVE ID : CVE-2023-32233**	https://github.com/torvalds/linux/commit/c1592a89942e9678f7d9c8030efa777c0d57edab, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c1592a89942e9678f7d9c8030efa777c0d57edab	O-RED-ENTE-170523/2838
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow	https://github.com/torvalds/linux/commit/67d7d8ad99be	O-RED-ENTE-170523/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a privileged local user to cause a system crash or other undefined behaviors. **CVE ID : CVE-2023-2513**		
Affected Version(s): 8.0					
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled. **CVE ID : CVE-2023-32233**	https://github.com/torvalds/linux/commit/c1592a89942e9678f7d9c8030efa777c0d57edab, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c1592a89942e9678f7d9c8030efa777c0d57edab	O-RED-ENTE-170523/2840
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. **CVE ID : CVE-2023-2513**	https://github.com/torvalds/linux/commit/67d7d8ad99be	O-RED-ENTE-170523/2841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.0					
Use After Free	08-May-2023	7.8	In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled. **CVE ID : CVE-2023-32233**	https://github.com/torvalds/linux/commit/c1592a89942e9678f7d9c8030efa777c0d57edab, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c1592a89942e9678f7d9c8030efa777c0d57edab	O-RED-ENTE-170523/2842
Use After Free	08-May-2023	6.7	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors. **CVE ID : CVE-2023-2513**	https://github.com/torvalds/linux/commit/67d7d8ad99be	O-RED-ENTE-170523/2843
Vendor: Rockwellautomation					
Product: armorstart_st_281e_firmware					
Affected Version(s): -					
Improper Neutralization of	11-May-2023	7.1	A cross site scripting vulnerability was	https://rockwellautomation.custhelp.c	O-ROC-ARMO-170523/2844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29030**	om/app/answers/answer_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29031		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29024**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2846
Improper Neutralization of Input During Web Page Generation	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29023**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29022		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29025**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2849
Improper Neutralization of Input During Web Page	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell	https://rockwellautomation.custhelp.com/app/answers/answe	O-ROC-ARMO-170523/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29026**	r_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29027**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29028		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29029**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2853
Product: armorstart_st_284ee_firmware					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell	https://rockwellautomation.custhelp.com/app/answers/answe	O-ROC-ARMO-170523/2854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29030**	r_view/a_id/1139438	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29031		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	6.5	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product A cross site scripting vulnerability was discovered that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29024**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2856
Improper Neutralization of Input During Web Page Generation	11-May-2023	6.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability. **CVE ID : CVE-2023-29023**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29022		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29025**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2859
Improper Neutralization of Input During Web Page Generation	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29026**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29027**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29028		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-May-2023	5.9	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user with admin privileges and network access to view user data and modify the web interface. Additionally, a malicious user could potentially cause interruptions to the availability of the web page. **CVE ID : CVE-2023-29029**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139438	O-ROC-ARMO-170523/2863
Vendor: Samsung					
Product: android					
Affected Version(s): 11.0					
Buffer Copy without Checking Size of Input	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_Plmncoordination.c in Shannon baseband prior to	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-170523/2864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21504**	r=2023&month=05	
Improper Authentication	04-May-2023	7.8	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation. **CVE ID : CVE-2023-21484**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2865
N/A	04-May-2023	7.8	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch arbitrary activity in Tips. **CVE ID : CVE-2023-21488**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2866
N/A	04-May-2023	7.1	Improper access control in GearManagerStub prior to SMR May-2023 Release 1 allows a local attacker to delete applications installed by watchmanager. **CVE ID : CVE-2023-21490**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-May-2023	6.8	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code. **CVE ID : CVE-2023-21489**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2868
N/A	04-May-2023	5.5	Improper access control vulnerability in SemShareFileProvider prior to SMR May-2023 Release 1 allows local attackers to access protected data. **CVE ID : CVE-2023-21493**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2869
N/A	04-May-2023	5.5	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set. **CVE ID : CVE-2023-21495**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2870
N/A	04-May-2023	5.5	Active Debug Code vulnerability in ActivityManagerService prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21496		
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in VideoPreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. **CVE ID : CVE-2023-21485**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2872
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in ImagePreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. **CVE ID : CVE-2023-21486**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2873
Insertion of Sensitive Information into Log File	04-May-2023	4.4	Kernel pointers are printed in the log file prior to SMR May-2023 Release 1 allows a privileged local attacker to bypass ASLR. **CVE ID : CVE-2023-21492**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-May-2023	3.3	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting. **CVE ID : CVE-2023-21487**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2875
Affected Version(s): 12.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_Plmncoordination.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21504**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2876
Improper Authentication	04-May-2023	7.8	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation. **CVE ID : CVE-2023-21484**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2877
N/A	04-May-2023	7.8	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch	https://security.samsungmobile.com/securityUpdate.smsb?yea	O-SAM-ANDR-170523/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary activity in Tips. **CVE ID : CVE-2023-21488**	r=2023&month=05	
N/A	04-May-2023	7.8	Improper access control vulnerability in ThemeManager prior to SMR May-2023 Release 1 allows local attackers to write arbitrary files with system privilege. **CVE ID : CVE-2023-21491**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2879
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in FactoryTest application prior to SMR May-2023 Release 1 allows local attackers to get privilege escalation via debugging commands. **CVE ID : CVE-2023-21502**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2880
N/A	04-May-2023	7.1	Improper access control in GearManagerStub prior to SMR May-2023 Release 1 allows a local attacker to delete applications installed by watchmanager. **CVE ID : CVE-2023-21490**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-May-2023	6.8	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code. **CVE ID : CVE-2023-21489**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2882
N/A	04-May-2023	5.5	Improper access control vulnerability in SemShareFileProvider prior to SMR May-2023 Release 1 allows local attackers to access protected data. **CVE ID : CVE-2023-21493**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2883
N/A	04-May-2023	5.5	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set. **CVE ID : CVE-2023-21495**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2884
N/A	04-May-2023	5.5	Active Debug Code vulnerability in ActivityManagerService prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21496		
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in VideoPreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. **CVE ID : CVE-2023-21485**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2886
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in ImagePreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. **CVE ID : CVE-2023-21486**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2887
Insertion of Sensitive Information into Log File	04-May-2023	4.4	Kernel pointers are printed in the log file prior to SMR May-2023 Release 1 allows a privileged local attacker to bypass ASLR. **CVE ID : CVE-2023-21492**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-May-2023	3.3	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting. **CVE ID : CVE-2023-21487**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2889
Affected Version(s): 13.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21494**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2890
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-May-2023	9.8	Potential buffer overflow vulnerability in mm_LteInterRatManagement.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21503**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2891
Buffer Copy without	04-May-2023	9.8	Potential buffer overflow vulnerability in	https://security.samsungmobile.com/	O-SAM-ANDR-170523/2892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			mm_Plmncoordination.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access. **CVE ID : CVE-2023-21504**	securityUpdate.smsb?year=2023&month=05	
Improper Authentication	04-May-2023	7.8	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation. **CVE ID : CVE-2023-21484**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2893
N/A	04-May-2023	7.8	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch arbitrary activity in Tips. **CVE ID : CVE-2023-21488**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2894
N/A	04-May-2023	7.8	Improper access control vulnerability in ThemeManager prior to SMR May-2023 Release 1 allows local attackers to write arbitrary files with system privilege.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21491		
Use of Externally-Controlled Format String	04-May-2023	7.8	Use of externally-controlled format string vulnerability in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to access the memory address. **CVE ID : CVE-2023-21497**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2896
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in setPartnerTAInfo in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to overwrite the trustlet memory. **CVE ID : CVE-2023-21498**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2897
Out-of-bounds Write	04-May-2023	7.8	Out-of-bounds write vulnerability in TA_Communication_mpos_encrypt_pin in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-21499**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2898
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in mPOS fiserve trustlet	https://security.samsungmobile.com/securityUpd	O-SAM-ANDR-170523/2899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to SMR May-2023 Release 1 allows local attackers to execute arbitrary code. **CVE ID : CVE-2023-21501**	ate.smsb?year=2023&month=05	
Improper Input Validation	04-May-2023	7.8	Improper input validation vulnerability in FactoryTest application prior to SMR May-2023 Release 1 allows local attackers to get privilege escalation via debugging commands. **CVE ID : CVE-2023-21502**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2900
N/A	04-May-2023	7.1	Improper access control in GearManagerStub prior to SMR May-2023 Release 1 allows a local attacker to delete applications installed by watchmanager. **CVE ID : CVE-2023-21490**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2901
Out-of-bounds Write	04-May-2023	6.8	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code. **CVE ID : CVE-2023-21489**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-May-2023	5.5	Improper access control vulnerability in SemShareFileProvider prior to SMR May-2023 Release 1 allows local attackers to access protected data. **CVE ID : CVE-2023-21493**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2903
N/A	04-May-2023	5.5	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set. **CVE ID : CVE-2023-21495**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2904
N/A	04-May-2023	5.5	Active Debug Code vulnerability in ActivityManagerService prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level. **CVE ID : CVE-2023-21496**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2905
Double Free	04-May-2023	5.5	Double free validation vulnerability in setPinPadImages in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to access the trustlet memory.	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21500		
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in VideoPreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. **CVE ID : CVE-2023-21485**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2907
N/A	04-May-2023	4.6	Improper export of android application components vulnerability in ImagePreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox. **CVE ID : CVE-2023-21486**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2908
Insertion of Sensitive Information into Log File	04-May-2023	4.4	Kernel pointers are printed in the log file prior to SMR May-2023 Release 1 allows a privileged local attacker to bypass ASLR. **CVE ID : CVE-2023-21492**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-May-2023	3.3	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting. **CVE ID : CVE-2023-21487**	https://security.samsungmobile.com/securityUpdate.smsb?year=2023&month=05	O-SAM-ANDR-170523/2910
Product: exynos_1080_firmware					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-170523/2911
Product: exynos_5123_firmware					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080.	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-170523/2912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**		
Product: exynos_5300_firmware					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-170523/2913
Product: exynos_980_firmware					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	09-May-2023	7.8	An issue was discovered in Exynos Mobile Processor and Modem for Exynos Modem 5123, Exynos Modem 5300, Exynos 980, and Exynos 1080. Binding of a wrong	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-170523/2914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource can occur due to improper handling of parameters while binding a network interface. **CVE ID : CVE-2023-29092**		
Vendor: shapeshift					
Product: keepkey_firmware					
Affected Version(s): From (including) 7.5.2 Up to (excluding) 7.7.0					
Out-of-bounds Read	02-May-2023	5.7	Insufficient length checks in the ShapeShift KeepKey hardware wallet firmware before 7.7.0 allow a global buffer overflow via crafted messages. Flaws in cf_confirmExecTx() in ethereum_contracts.c can be used to reveal arbitrary microcontroller memory on the device screen or crash the device. With physical access to a PIN-unlocked device, attackers can extract the BIP39 mnemonic secret from the hardware wallet. **CVE ID : CVE-2023-27892**	https://github.com/keepkey/keepkey-firmware/pull/337	O-SHA-KEEP-170523/2915
Vendor: Siemens					
Product: 6gk1411-1ac00_firmware					
Affected Version(s): * Up to (excluding) 2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Standardized Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). **CVE ID : CVE-2023-29105**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2916
Use of Hard-coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. **CVE ID : CVE-2023-29103**		
Affected Version(s): 2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to.	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29104		
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint. **CVE ID : CVE-2023-29106**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2919
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges. **CVE ID : CVE-2023-28832**		
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources. **CVE ID : CVE-2023-29107**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2921
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated privileged remote attacker to write any file with the extension `.db`. **CVE ID : CVE-2023-29128**		
Product: 6gk1411-5ac00_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Missing Standardized Error Handling Mechanism	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device is vulnerable to a denial of service while parsing a random (non-JSON) MQTT payload. This could allow an attacker who can manipulate the communication between the MQTT broker and the affected device to cause a denial of service (DoS). **CVE ID : CVE-2023-29105**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Password	09-May-2023	4.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC712 (All versions < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions < V2.1). The affected device uses a hard-coded password to protect the diagnostic files. This could allow an authenticated attacker to access protected data. **CVE ID : CVE-2023-29103**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2924
Affected Version(s): 2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	7.6	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated privileged remote attacker to overwrite any file the Linux user `ccuser` has write access to, or to download any file the Linux user `ccuser` has read-only access to. **CVE ID : CVE-2023-29104**		
Exposure of Sensitive Information to an Unauthorized Actor	09-May-2023	7.5	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint is accessible via REST API without authentication. This could allow an unauthenticated remote attacker to download the files available via the endpoint. **CVE ID : CVE-2023-29106**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2926
Improper Neutralization of Special Elements used in a Command ('Comman	09-May-2023	7.2	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			web based management of affected devices does not properly validate user input, making it susceptible to command injection. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges. **CVE ID : CVE-2023-28832**		
Files or Directories Accessible to External Parties	09-May-2023	5.3	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7 CC716 (All versions >= V2.0 < V2.1). The export endpoint discloses some undocumented files. This could allow an unauthenticated remote attacker to gain access to additional information resources. **CVE ID : CVE-2023-29107**	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2928
Improper Limitation of a Pathname to a Restricted Directory	09-May-2023	2.7	A vulnerability has been identified in SIMATIC Cloud Connect 7 CC712 (All versions >= V2.0 < V2.1), SIMATIC Cloud Connect 7	https://cert-portal.siemens.com/productcert/pdf/ssa-555292.pdf	O-SIE-6GK1-170523/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			CC716 (All versions >= V2.0 < V2.1). The filename in the upload feature of the web based management of the affected device is susceptible to a path traversal vulnerability. This could allow an authenticated privileged remote attacker to write any file with the extension `.db`. **CVE ID : CVE-2023-29128**		
Product: scalance_lpe9403_firmware					
Affected Version(s): * Up to (excluding) 2.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-May-2023	9.9	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user. **CVE ID : CVE-2023-27407**	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	O-SIE-SCAL-170523/2930
Creation of Temporary	09-May-2023	3.3	A vulnerability has been identified in	https://cert-portal.sieme	O-SIE-SCAL-170523/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File With Insecure Permissions			SCALANCE LPE9403 (All versions < V2.1). The `i2c` mutex file is created with the permissions bits of `-rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects. **CVE ID : CVE-2023-27408**	ns.com/productcert/pdf/ssa-325383.pdf	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-May-2023	3.3	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`. **CVE ID : CVE-2023-27409**	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	O-SIE-SCAL-170523/2932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Heap-based Buffer Overflow	09-May-2023	2.7	A vulnerability has been identified in SCALANCE LPE9403 (All versions < V2.1). A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service. **CVE ID : CVE-2023-27410**	https://cert-portal.siemens.com/productcert/pdf/ssa-325383.pdf	O-SIE-SCAL-170523/2933
Vendor: spryker					
Product: commerce_os					
Affected Version(s): 0.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-May-2023	8.8	SQL injection vulnerability inSpryker Commerce OS 0.9 that allows for access to sensitive data via customer/order?ordersearchForm[searchText]= **CVE ID : CVE-2023-27568**	N/A	O-SPR-COMM-170523/2934
Vendor: Tenda					
Product: ac18_firmware					
Affected Version(s): 15.03.05.19\\(6318\\)_cn					
Improper Neutralization of	05-May-2023	9.8	Tenda AC18 v15.03.05.19(6318_)_cn was discovered	https://github.com/DrizzlingSun/Tend	O-TEN-AC18-170523/2935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			to contain a command injection vulnerability via the deviceName parameter in the setUsbUnload function. **CVE ID : CVE-2023-30135**	a/blob/main/AC18/8/8.md	
Product: n301_firmware					
Affected Version(s): 12.02.01.61_multi					
Cleartext Transmission of Sensitive Information	01-May-2023	5.7	Cleartext Transmission in cookie:ecos_pw: in Tenda N301 v6.0, firmware v12.03.01.06_pt allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password. **CVE ID : CVE-2023-29681**	N/A	O-TEN-N301-170523/2936
Affected Version(s): 12.03.01.06_pt					
Cleartext Transmission of Sensitive Information	01-May-2023	5.7	Cleartext Transmission in set-cookie:ecos_pw: Tenda N301 v6.0, Firmware v12.02.01.61_multi allows an authenticated attacker on the LAN or WLAN to intercept communications with the router and obtain the password.	N/A	O-TEN-N301-170523/2937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29680		
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191024 is vulnerable to Command Injection. **CVE ID : CVE-2023-30053**	N/A	O-TOT-A710-170523/2938
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK A7100RU V7.4cu.2313_B20191024 has a Command Injection vulnerability. An attacker can obtain a stable root shell through a specially constructed payload. **CVE ID : CVE-2023-30054**	N/A	O-TOT-A710-170523/2939
Product: x5000r_firmware					
Affected Version(s): 9.1.0u.6118_b20201102					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and V9.1.0u.6369_B20230113 contain a command insertion vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary	N/A	O-TOT-X500-170523/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands through the "command" parameter. **CVE ID : CVE-2023-30013**		
Affected Version(s): 9.1.0u.6369_b20230113					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-May-2023	9.8	TOTOLINK X5000R V9.1.0u.6118_B20201102 and V9.1.0u.6369_B20230113 contain a command insertion vulnerability in setting/setTracerouteCfg. This vulnerability allows an attacker to execute arbitrary commands through the "command" parameter. **CVE ID : CVE-2023-30013**	N/A	O-TOT-X500-170523/2941
Vendor: Zyxel					
Product: nbg-418n_firmware					
Affected Version(s): * Up to (including) 1.00\\(aarp.13\\)c0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-May-2023	7.5	A cross-site scripting (XSS) vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to store malicious scripts using a web management interface parameter,	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	O-ZYX-NBG--170523/2942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in denial-of-service (DoS) conditions on an affected device. **CVE ID : CVE-2023-22921**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-May-2023	7.5	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote unauthenticated attacker to cause DoS conditions by sending crafted packets if Telnet is enabled on a vulnerable device. **CVE ID : CVE-2023-22922**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	O-ZYX-NBG--170523/2943
Use of Externally-Controlled Format String	01-May-2023	6.5	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker to cause denial-of-service (DoS) conditions on an affected device. **CVE ID : CVE-2023-22923**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	O-ZYX-NBG--170523/2944
Buffer Copy without Checking Size of	01-May-2023	4.9	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to	https://www.zyxel.com/global/en/support/security-	O-ZYX-NBG--170523/2945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing crafted CLI commands on a vulnerable device. **CVE ID : CVE-2023-22924**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router	
Product: nbg6604_firmware					
Affected Version(s): 1.01\\(abir.0\\)c0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-May-2023	8.8	The post-authentication command injection vulnerability in the Zyxel NBG6604 firmware version V1.01(ABIR.0)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request. **CVE ID : CVE-2023-22919**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-nbg6604-home-router	O-ZYX-NBG6-170523/2946