National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 – 30 Apr 2023 Vol. 10 No. 08

Table of Content

Vendor	Product	Page Number
codedropz	drag_and_drop_multiple_file_upload_-_contact_form_7	20
coderex	wp_vr	21
codesector	teracopy	21
complaint_management_system_project	complaint_management_system	22
Dedecms	dedecms	22
Dell	display_manager	23
devolutions	devolutions_server	23
digitalblue	click_to_call_or_chat_buttons	24
dircms_project	dircms	24
discourse	discourse	24
dogecoin	dogecoin	45
Eclipse	jetty	46
egostudiogroup	super_clean	56
electra-air	smart_kit_for_split_ac	57
electric_studio_client_login_project	electric_studio_client_login	57
encode	starlette	57
faturamatik	bircard	58
freesoul_deactivate_plugins_-_plugin_manager_and_cleanup_project	freesoul_deactivate_plugins_-_plugin_manager_and_cleanup	58
fullworksplugins	quick_paypal_payments	59
gatsbyjs	gatsby	59
gipsy_project	gipsy	62
Google	chrome	63
google_maps_v3_shortcode_project	google_maps_v3_shortcode	65
i13websolution	responsive_filterable_portfolio	65
	thumbnail_carousel_slider	66
inisev	redirection	67

Vendor	Product	Page Number
Juniper	acx1000	425
	acx1100	428
	acx2000	431
	acx2100	433
	acx2200	436
	acx4000	439
	acx500	441
	acx5000	444
	acx5048	447
	acx5096	449
	acx5400	452
	acx5448	455
	acx5800	457
	acx6300	460
	acx6360	463
	acx710	465
	acx7100-32c	468
	acx7100-48l	471
	acx7509	473
	jrr200	476
	mx	477
	mx10	479
	mx10000	480
	mx10003	482
	mx10008	483
	mx10016	485
	mx104	486
	mx150	488
	mx2008	490
	mx2010	491
	mx2020	493
	mx204	494

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: photo_gallery					
Affected Version(s): * Up to (excluding) 1.8.15					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Apr-2023	4.9	- The Photo Gallery by 10Web WordPress plugin before 1.8.15 did not ensure that uploaded files are kept inside its uploads folder, allowing high privilege users to put images anywhere in the filesystem via a path traversal vector. **CVE ID : CVE-2023-1427**	N/A	A-10W-PHOT-030523/1
Vendor: 71note					
Product: go-bbs					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	8.8	go-bbs v1 was discovered to contain an arbitrary file download vulnerability via the component /api/v1/download. **CVE ID : CVE-2023-27755**	N/A	A-71N-GO-B-030523/2
Vendor: air_cargo_management_system_project					
Product: air_cargo_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During	18-Apr-2023	4.8	A vulnerability was found in SourceCodester Air Cargo Management System 1.0. It has been	N/A	A-AIR-AIR_-030523/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			declared as problematic. This vulnerability affects unknown code of the file classes/Master.php?f=save_cargo_type. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226276. **CVE ID : CVE-2023-2155**		
Vendor: ai_contact_us_form_project					
Product: ai_contact_us_form					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Karishma Arora AI Contact Us Form plugin <= 1.0 versions. **CVE ID : CVE-2023-24386**	N/A	A-AI_-AI_C-030523/4
Vendor: altran					
Product: picotcp					
Affected Version(s): * Up to (including) 1.7.0					
Integer Overflow or Wraparound	19-Apr-2023	7.5	Altran picoTCP through 1.7.0 allows memory corruption (and subsequent denial of service) because of an integer	N/A	A-ALT-PICO-030523/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in pico_ipv6_alloc when processing large ICMPv6 packets. This affects installations with Ethernet support in which a packet size greater than 65495 may occur. **CVE ID : CVE-2023-30463**		
Vendor: Apache					
Product: iotdb					
Affected Version(s): 0.13.3					
Incorrect Authorization	17-Apr-2023	9.8	Incorrect Authorization vulnerability in Apache Software Foundation Apache IoTDB.This issue affects the iotdb-web-workbench component on 0.13.3. iotdb-web-workbench is an optional component of IoTDB, providing a web console of the database. This problem is fixed from version 0.13.4 of iotdb-web-workbench onwards. **CVE ID : CVE-2023-30771**	https://lists.apache.org/thread/08nc3dr6lshfppx0pzmz5vbggdnzpojb	A-APA-IOTD-030523/6
Affected Version(s): From (including) 0.13.0 Up to (including) 0.13.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Apr-2023	9.8	Improper Authentication vulnerability in Apache Software Foundation Apache IoTDB.This issue affects Apache IoTDB Grafana Connector: from 0.13.0 through 0.13.3. Attackers could login without authorization. This is fixed in 0.13.4. **CVE ID : CVE-2023-24831**	https://lists.apache.org/thread/3dgvzgstycf8b5hyf4z3n7cqdhcyln3l	A-APA-IOTD-030523/7
Product: spark					
Affected Version(s): * Up to (excluding) 3.4.0					
Improper Privilege Management	17-Apr-2023	9.9	In Apache Spark versions prior to 3.4.0, applications using spark-submit can specify a 'proxy-user' to run as, limiting privileges. The application can execute code with the privileges of the submitting user, however, by providing malicious configuration-related classes on the classpath. This affects architectures relying on proxy-user, for example those using Apache Livy to manage submitted applications.	https://lists.apache.org/thread/yllfl25xh5tbotjmg93zrq4bzwhqc0gv	A-APA-SPAR-030523/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Update to Apache Spark 3.4.0 or later, and ensure that spark.submit.proxyUser.allowCustomClasspathInClusterMode is set to its default of "false", and is not overridden by submitted applications. **CVE ID : CVE-2023-22946**		
Product: superset					
Affected Version(s): * Up to (including) 2.0.1					
Server-Side Request Forgery (SSRF)	17-Apr-2023	6.5	A malicious actor who has been authenticated and granted specific permissions in Apache Superset may use the import dataset feature in order to conduct Server-Side Request Forgery attacks and query internal resources on behalf of the server where Superset is deployed. This vulnerability exists in Apache Superset versions up to and including 2.0.1.	N/A	A-APA-SUPE-030523/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25504		
Incorrect Authorization	17-Apr-2023	4.3	An authenticated user with Gamma role authorization could have access to metadata information using non trivial methods in Apache Superset up to and including 2.0.1 **CVE ID : CVE-2023-27525**	https://lists.apache.org/thread/wpv7b17zjg2pmvpfkdd6nn8sco8y2q77	A-APA-SUPE-030523/10
Vendor: apng_optimizer_project					
Product: apng_optimizer					
Affected Version(s): 1.4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Apr-2023	7.5	APNG_Optimizer v1.4 was discovered to contain a buffer overflow via the component /apngopt/ubuntu.png. **CVE ID : CVE-2023-27705**	N/A	A-APN-APNG-030523/11
Vendor: archerydms					
Product: archery					
Affected Version(s): 1.9.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Apr-2023	6.5	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. User input coming	https://github.com/hhyo/Archery/security/advisories/GHSA-jwjj-jgfv-x66q	A-ARC-ARCH-030523/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the `db_name` in the `sql/data_dictionary.py` `table_list` endpoint is passed to the methods that follow in a given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution. The affected methods are `get_group_tables_by_db` in `sql/engines/mssql.py `which passes unsafe user input to `sql/engines/mssql.py`, and `get_group_tables_by_db` in `sql/engines/oracle.py `which concatenates input which is passed to execution on the database in the `sql/engines/oracle.py` `query` method. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This issue is also indexed as `GHSL-2022-105`. **CVE ID : CVE-2023-30558**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Apr-2023	6.5	Archery is an open source SQL audit platform. The Archery project contains multiple SQL injection vulnerabilities, that may allow an attacker to query the connected databases. User input coming from the `variable_name` and `variable_value` parameter value in the `sql/instance.py` `param_edit` endpoint is passed to a set of methods in given SQL engine implementations, which concatenate user input unsafely into a SQL query and afterwards pass it to the `query` method of each database engine for execution. The affected methods are: `set_variable` in `sql/engines/goinception.py` which concatenates input which is passed to execution on the database in the `sql/engines/goinception.py`, `get_variables` in `sql/engines/goinception.py` which concatenates input which is passed to execution on the database in the	https://github.com/hhyo/Archery/security/advisories/GHSA-6mqc-w2qp-fvhp	A-ARC-ARCH-030523/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`sql/engines/goinception.py`, `set_variable` in `sql/engines/mysql.py` which concatenates input which is passed to execution on the database in the `sql/engines/mysql.py` `query`, and `get_variables` in `sql/engines/mysql.py` which concatenates input which is passed to execution on the database in the `sql/engines/mysql.py` `query`. Each of these issues may be mitigated by escaping user input or by using prepared statements when executing SQL queries. This advisory is also indexed as `GHSL-2022-104`. **CVE ID : CVE-2023-30605**		
Vendor: archivist_-_custom_archive_templates_project					
Product: archivist_-_custom_archive_templates					
Affected Version(s): * Up to (excluding) 1.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eric Teubert Archivist – Custom Archive Templates plugin <= 1.7.4 versions. **CVE ID : CVE-2023-25490**	N/A	A-ARC-ARCH-030523/14
Vendor: Asustor					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: adm					
Affected Version(s): From (including) 4.0.0.rib4 Up to (including) 4.0.6.reg2					
Out-of-bounds Write	17-Apr-2023	9.8	A stack-based buffer overflow vulnerability was found in the ASUSTOR Data Master (ADM) due to the lack of data size validation. An attacker can exploit this vulnerability to execute arbitrary code. Affected ADM versions include: 4.0.6.REG2, 4.1.0 and below as well as 4.2.0.RE71 and below. **CVE ID : CVE-2023-30770**	https://www.asustor.com/security/security_advisory_detail?id=21	A-ASU-ADM-030523/15
Affected Version(s): From (including) 4.1.0.rhu2 Up to (excluding) 4.2.1.rge2					
Out-of-bounds Write	17-Apr-2023	9.8	A stack-based buffer overflow vulnerability was found in the ASUSTOR Data Master (ADM) due to the lack of data size validation. An attacker can exploit this vulnerability to execute arbitrary code. Affected ADM versions include: 4.0.6.REG2, 4.1.0 and below as well as 4.2.0.RE71 and below. **CVE ID : CVE-2023-30770**	https://www.asustor.com/security/security_advisory_detail?id=21	A-ASU-ADM-030523/16
Vendor: Autodesk					
Product: fbx_software_development_kit					
Affected Version(s): From (including) 2020.0 Up to (excluding) 2020.3.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Apr-2023	7.8	An Out-Of-Bounds Write Vulnerability in Autodesk® FBX® SDK version 2020 or prior may lead to code execution through maliciously crafted FBX files or information disclosure. **CVE ID : CVE-2023-27909**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0004	A-AUT-FBX_-030523/17
Out-of-bounds Write	17-Apr-2023	7.8	A user may be tricked into opening a malicious FBX file that may exploit a stack buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior which may lead to code execution. **CVE ID : CVE-2023-27910**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0004	A-AUT-FBX_-030523/18
Out-of-bounds Write	17-Apr-2023	7.8	A user may be tricked into opening a malicious FBX file that may exploit a heap buffer overflow vulnerability in Autodesk® FBX® SDK 2020 or prior which may lead to code execution. **CVE ID : CVE-2023-27911**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0004	A-AUT-FBX_-030523/19
Product: maya_usd					
Affected Version(s): * Up to (excluding) 0.23.0					
Improper Initialization	17-Apr-2023	7.8	A malicious actor may convince a victim to open a malicious USD	https://www.autodesk.com/trust/se	A-AUT-MAYA-030523/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file that may trigger an uninitialized variable which may result in code execution. **CVE ID : CVE-2023-25010**	curity-advisories/adsk-sa-2023-0003	
Out-of-bounds Read	17-Apr-2023	7.8	A malicious actor may convince a victim to open a malicious USD file that may trigger an out-of-bounds read vulnerability which may result in code execution. **CVE ID : CVE-2023-27906**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0003	A-AUT-MAYA-030523/21
Out-of-bounds Write	17-Apr-2023	7.8	A malicious actor may convince a victim to open a malicious USD file that may trigger an out-of-bounds write vulnerability which may result in code execution. **CVE ID : CVE-2023-27907**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0003	A-AUT-MAYA-030523/22
Vendor: Avast					
Product: antivirus					
Affected Version(s): From (including) 22.5 Up to (excluding) 22.11					
NULL Pointer Dereference	19-Apr-2023	5.5	Avast and AVG Antivirus for Windows were susceptible to a NULL pointer dereference issue via RPC-interface. The issue was fixed with Avast and AVG Antivirus version 22.11	N/A	A-AVA-ANTI-030523/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1587		
Vendor: AVG					
Product: anti-virus					
Affected Version(s): From (including) 22.5 Up to (excluding) 22.11					
NULL Pointer Dereference	19-Apr-2023	5.5	Avast and AVG Antivirus for Windows were susceptible to a NULL pointer dereference issue via RPC-interface. The issue was fixed with Avast and AVG Antivirus version 22.11 **CVE ID : CVE-2023-1587**	N/A	A-AVG-ANTI-030523/24
Vendor: Avira					
Product: antivirus					
Affected Version(s): * Up to (excluding) 1.0.2303.633					
Integer Overflow or Wraparound	19-Apr-2023	5.5	A vulnerability within the Avira network protection feature allowed an attacker with local execution rights to cause an overflow. This could corrupt the data on the heap and lead to a denial-of-service situation. Issue was fixed with Endpointprotection.exe version 1.0.2303.633 **CVE ID : CVE-2023-1900**	N/A	A-AVI-ANTI-030523/25
Vendor: azuracast					
Product: azuracast					
Affected Version(s): * Up to (excluding) 0.18.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository azuracast/azuracast prior to 0.18. **CVE ID : CVE-2023-2191**	https://github.com/azuracast/azuracast/commit/24276cb4166b2057de73569ec33046a80a8bb437, https://huntr.dev/bounties/0814f5f9-8b58-40e5-b08c-7c488947cf31	A-AZU-AZUR-030523/26
Vendor: Bestwebsoft					
Product: gallery					
Affected Version(s): * Up to (excluding) 4.7.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2023	8.8	The Gallery by BestWebSoft WordPress plugin before 4.7.0 does not properly escape values used in SQL queries, leading to an Blind SQL Injection vulnerability. The attacker must have at least the privileges of an Author, and the vendor's Slider plugin (https://wordpress.org/plugins/slider-bws/) must also be installed for this vulnerability to be exploitable. **CVE ID : CVE-2023-0765**	N/A	A-BES-GALL-030523/27
Improper Neutralization of	17-Apr-2023	5.4	The Gallery by BestWebSoft WordPress plugin	N/A	A-BES-GALL-030523/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			before 4.7.0 does not perform proper sanitization of gallery information, leading to a Stored Cross-Site Scription vulnerability. The attacker must have at least the privileges of the Author role. **CVE ID : CVE-2023-0764**		
Vendor: Cesanta					
Product: mjs					
Affected Version(s): 2.20.0					
N/A	24-Apr-2023	5.5	Cesanta MJS v2.20.0 was discovered to contain a SEGV vulnerability via mjs_ffi_cb_free at src/mjs_ffi.c. This vulnerability can lead to a Denial of Service (DoS). **CVE ID : CVE-2023-29570**	N/A	A-CES-MJS-030523/29
Vendor: chatwoot					
Product: chatwoot					
Affected Version(s): * Up to (excluding) 2.14.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	6.1	Cross-site Scripting (XSS) - DOM in GitHub repository chatwoot/chatwoot prior to 2.14.0. **CVE ID : CVE-2023-2109**	https://github.com/chatwoot/chatwoot/commit/a06a5a574ad908b0ef2db7b47d05c3774eeb493d, https://huntr.dev/bounties/fd5999fd-b1fd-44b4-	A-CHA-CHAT-030523/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ae2e-8f95b5c3d1b6	
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): 4.5.3					
Improper Neutralization of Formula Elements in a CSV File	25-Apr-2023	7.8	ChurchCRM 4.5.3 was discovered to contain a CSV injection vulnerability via the Last Name and First Name input fields when creating a new person. These vulnerabilities allow attackers to execute arbitrary code via a crafted excel file. **CVE ID : CVE-2023-25348**	N/A	A-CHU-CHUR-030523/31
Cross-Site Request Forgery (CSRF)	25-Apr-2023	6.5	A cross-site request forgery (CSRF) vulnerability in ChurchCRM v4.5.3 allows attackers to change any user's password except for the user that is currently logged in. **CVE ID : CVE-2023-26841**	https://github.com/ChurchCRM/CRM	A-CHU-CHUR-030523/32
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in ChurchCRM 4.5.3 allows remote attackers to inject arbitrary web script or HTML via the id parameter of	N/A	A-CHU-CHUR-030523/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/churchcrm/v2/family/not-found. **CVE ID : CVE-2023-25346**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	5.4	A stored cross-site scripting (XSS) vulnerability in ChurchCRM 4.5.3, allows remote attackers to inject arbitrary web script or HTML via input fields. These input fields are located in the "Title" Input Field in EventEditor.php. **CVE ID : CVE-2023-25347**	N/A	A-CHU-CHUR-030523/34
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	5.4	A stored Cross-site scripting (XSS) vulnerability in ChurchCRM 4.5.3 allows remote attackers to inject arbitrary web script or HTML via the NoteEditor.php. **CVE ID : CVE-2023-26843**	N/A	A-CHU-CHUR-030523/35
Cross-Site Request Forgery (CSRF)	25-Apr-2023	5.3	A cross-site request forgery (CSRF) vulnerability in ChurchCRM v4.5.3 allows attackers to set a person to a user and set that user to be an Administrator. **CVE ID : CVE-2023-26840**	N/A	A-CHU-CHUR-030523/36
Cross-Site Request	25-Apr-2023	4.3	A cross-site request forgery (CSRF)	N/A	A-CHU-CHUR-030523/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerability in ChurchCRM v4.5.3 allows attackers to edit information for existing people on the site. **CVE ID : CVE-2023-26839**		
Vendor: cloverdx					
Product: cloverdx					
Affected Version(s): 5.16.0					
Insertion of Sensitive Information into Log File	24-Apr-2023	6.5	CloverDX before 5.17.3 writes passwords to the audit log in certain situations, if the audit log is enabled and single sign-on is not employed. The fixed versions are 5.15.4, 5.16.2, 5.17.3, and 6.0.x. **CVE ID : CVE-2023-31056**	https://support1.cloverdx.com/hc/en-us/articles/8484869595164-Security-advisory-April-2023	A-CLO-CLOV-030523/38
Affected Version(s): 5.16.1					
Insertion of Sensitive Information into Log File	24-Apr-2023	6.5	CloverDX before 5.17.3 writes passwords to the audit log in certain situations, if the audit log is enabled and single sign-on is not employed. The fixed versions are 5.15.4, 5.16.2, 5.17.3, and 6.0.x. **CVE ID : CVE-2023-31056**	https://support1.cloverdx.com/hc/en-us/articles/8484869595164-Security-advisory-April-2023	A-CLO-CLOV-030523/39
Affected Version(s): From (including) 5.14.0 Up to (including) 5.14.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	24-Apr-2023	6.5	CloverDX before 5.17.3 writes passwords to the audit log in certain situations, if the audit log is enabled and single sign-on is not employed. The fixed versions are 5.15.4, 5.16.2, 5.17.3, and 6.0.x. **CVE ID : CVE-2023-31056**	https://support1.cloverdx.com/hc/en-us/articles/8484869595164-Security-advisory-April-2023	A-CLO-CLOV-030523/40
Affected Version(s): From (including) 5.15.0 Up to (including) 5.15.3					
Insertion of Sensitive Information into Log File	24-Apr-2023	6.5	CloverDX before 5.17.3 writes passwords to the audit log in certain situations, if the audit log is enabled and single sign-on is not employed. The fixed versions are 5.15.4, 5.16.2, 5.17.3, and 6.0.x. **CVE ID : CVE-2023-31056**	https://support1.cloverdx.com/hc/en-us/articles/8484869595164-Security-advisory-April-2023	A-CLO-CLOV-030523/41
Affected Version(s): From (including) 5.17.0 Up to (excluding) 5.17.3					
Insertion of Sensitive Information into Log File	24-Apr-2023	6.5	CloverDX before 5.17.3 writes passwords to the audit log in certain situations, if the audit log is enabled and single sign-on is not employed. The fixed versions are 5.15.4, 5.16.2, 5.17.3, and 6.0.x. **CVE ID : CVE-2023-31056**	https://support1.cloverdx.com/hc/en-us/articles/8484869595164-Security-advisory-April-2023	A-CLO-CLOV-030523/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: codedropz					
Product: drag_and_drop_multiple_file_upload_-_contact_form_7					
Affected Version(s): * Up to (excluding) 2.11.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	6.1	The Drag and Drop Multiple File Upload PRO - Contact Form 7 Standard WordPress plugin before 2.11.1 and Drag and Drop Multiple File Upload PRO - Contact Form 7 with Remote Storage Integrations WordPress plugin before 5.0.6.4 do not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high-privilege users such as admins. **CVE ID : CVE-2023-1282**	N/A	A-COD-DRAG-030523/43
Affected Version(s): * Up to (excluding) 5.0.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	6.1	The Drag and Drop Multiple File Upload PRO - Contact Form 7 Standard WordPress plugin before 2.11.1 and Drag and Drop Multiple File Upload PRO - Contact Form 7 with Remote Storage Integrations WordPress plugin before 5.0.6.4 do not sanitise and escape a parameter before outputting it back in	N/A	A-COD-DRAG-030523/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the page, leading to a Reflected Cross-Site Scripting which could be used against high-privilege users such as admins. **CVE ID : CVE-2023-1282**		
Vendor: coderex					
Product: wp_vr					
Affected Version(s): * Up to (excluding) 8.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	6.1	The WP VR WordPress plugin before 8.2.9 does not sanitise and escape some parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-1413**	N/A	A-COD-WP_V-030523/45
Vendor: codesector					
Product: teracopy					
Affected Version(s): 3.9.7					
N/A	19-Apr-2023	6.5	Code Sector TeraCopy 3.9.7 does not perform proper access validation on the source folder during a copy operation. This leads to Arbitrary File Read by allowing any user to copy any directory in the system to a directory they control.	N/A	A-COD-TERA-030523/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29586		
Vendor: complaint_management_system_project					
Product: complaint_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	A vulnerability was found in SourceCodester Complaint Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file admin/assets/plugins/DataTables/examples/examples_support/editable_ajax.php of the component POST Parameter Handler. The manipulation of the argument value with the input 1><script>alert(666)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-226274 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2153**	N/A	A-COM-COMP-030523/47
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 5.7.106					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2023	7.2	DedeCMS v5.7.106 was discovered to contain a SQL injection vulnerability via the component /dede/sys_sql_query.php. **CVE ID : CVE-2023-27733**	N/A	A-DED-DEDE-030523/48
Vendor: Dell					
Product: display_manager					
Affected Version(s): * Up to (including) 2.1.0					
Least Privilege Violation	20-Apr-2023	7.8	Dell Display Manager, versions 2.1.0 and prior, contains an arbitrary file or folder creation vulnerability during installation. A local low privilege attacker could potentially exploit this vulnerability, leading to the execution of arbitrary code on the operating system with high privileges. **CVE ID : CVE-2023-28047**	https://www.dell.com/support/kbdoc/en-uk/000211727/dsa-2023	A-DEL-DISP-030523/49
Vendor: devolutions					
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2023.1.6.0					
N/A	21-Apr-2023	5.4	Insufficient access control in support ticket feature in Devolutions Server 2023.1.5.0 and	https://devolutions.net/security/advisories/DEVO-2023-0010	A-DEV-DEVO-030523/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below allows an authenticated attacker to send support tickets and download diagnostic files via specific endpoints. **CVE ID : CVE-2023-2118**		
Vendor: digitalblue					
Product: click_to_call_or_chat_buttons					
Affected Version(s): * Up to (excluding) 1.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in DIGITALBLUE Click to Call or Chat Buttons plugin <= 1.4.0 versions. **CVE ID : CVE-2023-25710**	N/A	A-DIG-CLIC-030523/51
Vendor: dircms_project					
Product: dircms					
Affected Version(s): 6.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	DirCMS 6.0.0 has a Cross Site Scripting (XSS) vulnerability in the foreground. **CVE ID : CVE-2023-29854**	N/A	A-DIR-DIRC-030523/52
Vendor: discourse					
Product: discourse					
Affected Version(s): 1.9.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected	https://github.com/discourse/discourse/security/	A-DIS-DISC-030523/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	advisories/GHSA-vm65-pv5h-6g3w	
Affected Version(s): * Up to (excluding) 3.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	Discourse is an open source platform for community discussion. This vulnerability is not exploitable on the default install of Discourse. A custom feature must be enabled for it to work at all, and the attacker's payload must pass the CSP to be executed. However, if an attacker succeeds in embedding Javascript that does pass the CSP, it could result in session hijacking for any users that view the	N/A	A-DIS-DISC-030523/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker's post. The vulnerability is patched in the latest tests-passed, beta and stable branches. Users are advised to upgrade. Users unable to upgrade should enable and/or restore your site's CSP to the default one provided with Discourse. Remove any embed-able hosts configured. **CVE ID : CVE-2023-29196**		
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/55
Affected Version(s): * Up to (excluding) 3.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	Discourse is an open source platform for community discussion. This vulnerability is not exploitable on the default install of Discourse. A custom feature must be enabled for it to work at all, and the attacker's payload must pass the CSP to be executed. However, if an attacker succeeds in embedding Javascript that does pass the CSP, it could result in session hijacking for any users that view the attacker's post. The vulnerability is patched in the latest tests-passed, beta and stable branches. Users are advised to upgrade. Users unable to upgrade should enable and/or restore your site's CSP to the default one provided with Discourse. Remove any embed-able hosts configured. **CVE ID : CVE-2023-29196**	N/A	A-DIS-DISC-030523/56
Improper Neutralization of Input During Web Page	18-Apr-2023	5.4	Discourse is an open source platform for community discussion. Due to the improper sanitization of SVG files, an	N/A	A-DIS-DISC-030523/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			attacker can execute arbitrary JavaScript on the users' browsers by uploading a crafted SVG file. This issue is patched in the latest stable and tests-passed versions of Discourse. Users are advised to upgrade. For users unable to upgrade there are two possible workarounds: enable CDN handing of uploads (and ensure the CDN sanitizes SVG files) or disable SVG file uploads by ensuring that the `authorized extensions` site setting does not include `svg` (or reset that setting to the default, by default Discourse doesn't enable SVG uploads by users). **CVE ID : CVE-2023-30538**		
Incorrect Permission Assignment for Critical Resource	18-Apr-2023	4.9	Discourse is an open source platform for community discussion. In affected versions a user logged as an administrator can call arbitrary methods on the `SiteSetting` class, notably `#clear_cache!` and `#notify_changed!`,	N/A	A-DIS-DISC-030523/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which when done on a multisite instance, can affect the entire cluster resulting in a denial of service. Users not running in multisite environments are not affected. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-30606**		
Affected Version(s): * Up to (including) 3.0.1					
Incorrect Permission Assignment for Critical Resource	18-Apr-2023	4.9	Discourse is an open source platform for community discussion. In affected versions a user logged as an administrator can call arbitrary methods on the `SiteSetting` class, notably `#clear_cache!` and `#notify_changed!`, which when done on a multisite instance, can affect the entire cluster resulting in a denial of service. Users not running in multisite environments are not affected. This issue is patched in the latest stable, beta and tests-	N/A	A-DIS-DISC-030523/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-30606**		
Affected Version(s): * Up to (including) 3.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	5.4	Discourse is an open source platform for community discussion. Due to the improper sanitization of SVG files, an attacker can execute arbitrary JavaScript on the users' browsers by uploading a crafted SVG file. This issue is patched in the latest stable and tests-passed versions of Discourse. Users are advised to upgrade. For users unable to upgrade there are two possible workarounds: enable CDN handing of uploads (and ensure the CDN sanitizes SVG files) or disable SVG file uploads by ensuring that the `authorized extensions` site setting does not include `svg` (or reset that setting to the default, by default Discourse doesn't	N/A	A-DIS-DISC-030523/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enable SVG uploads by users). **CVE ID : CVE-2023-30538**		
Affected Version(s): 1.1.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/61
Affected Version(s): 1.2.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 1.3.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/63
Affected Version(s): 1.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/64
Affected Version(s): 1.5.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 1.6.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/66
Affected Version(s): 1.7.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 1.8.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28440		
Affected Version(s): 2.0.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/69
Affected Version(s): 2.1.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 2.2.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/71
Affected Version(s): 2.3.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community	https://github.com/discourse/discour	A-DIS-DISC-030523/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	se/security/advisories/GHSA-vm65-pv5h-6g3w	
Affected Version(s): 2.4.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade.	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/73

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 2.5.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/74
Affected Version(s): 2.6.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 2.7.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/76
Affected Version(s): 2.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/77
Affected Version(s): 2.9.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**		
Affected Version(s): 3.0.0					
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/79
Affected Version(s): 3.1.0					
Improper Neutralization of Input During Web Page Generation	18-Apr-2023	6.1	Discourse is an open source platform for community discussion. This vulnerability is not exploitable on the default install of	N/A	A-DIS-DISC-030523/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Discourse. A custom feature must be enabled for it to work at all, and the attacker's payload must pass the CSP to be executed. However, if an attacker succeeds in embedding Javascript that does pass the CSP, it could result in session hijacking for any users that view the attacker's post. The vulnerability is patched in the latest tests-passed, beta and stable branches. Users are advised to upgrade. Users unable to upgrade should enable and/or restore your site's CSP to the default one provided with Discourse. Remove any embed-able hosts configured. **CVE ID : CVE-2023-29196**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	5.4	Discourse is an open source platform for community discussion. Due to the improper sanitization of SVG files, an attacker can execute arbitrary JavaScript on the users' browsers by uploading a crafted SVG file. This issue is patched in the latest stable and tests-	N/A	A-DIS-DISC-030523/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			passed versions of Discourse. Users are advised to upgrade. For users unable to upgrade there are two possible workarounds: enable CDN handing of uploads (and ensure the CDN sanitizes SVG files) or disable SVG file uploads by ensuring that the `authorized extensions` site setting does not include `svg` (or reset that setting to the default, by default Discourse doesn't enable SVG uploads by users). **CVE ID : CVE-2023-30538**		
Incorrect Permission Assignment for Critical Resource	18-Apr-2023	4.9	Discourse is an open source platform for community discussion. In affected versions a user logged as an administrator can call arbitrary methods on the `SiteSetting` class, notably `#clear_cache!` and `#notify_changed!`, which when done on a multisite instance, can affect the entire cluster resulting in a denial of service. Users not running in multisite	N/A	A-DIS-DISC-030523/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environments are not affected. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-30606**		
N/A	18-Apr-2023	2.7	Discourse is an open source platform for community discussion. In affected versions a maliciously crafted request from a Discourse administrator can lead to a long-running request and eventual timeout. This has the greatest potential impact in shared hosting environments where admins are untrusted. This issue has been addressed in versions 3.0.3 and 3.1.0.beta4. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28440**	https://github.com/discourse/discourse/security/advisories/GHSA-vm65-pv5h-6g3w	A-DIS-DISC-030523/83
Vendor: dogecoin					
Product: dogecoin					
Affected Version(s): * Up to (excluding) 1.14.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	9.8	Vulnerability discovered is related to the peer-to-peer (p2p) communications, attackers can craft consensus messages, send it to individual nodes and take them offline. An attacker can crawl the network peers using getaddr message and attack the unpatched nodes. **CVE ID : CVE-2023-30769**	N/A	A-DOG-DOGE-030523/84
Vendor: Eclipse					
Product: jetty					
Affected Version(s): * Up to (excluding) 9.4.51					
Allocation of Resources Without Limits or Throttling	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. In affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call `HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0`	https://github.com/eclipse/jetty.project/pull/9345, https://github.com/eclipse/jetty.project/pull/9344, https://github.com/eclipse/jetty.project/security/advisories/GHSA-qw69-rqj8-6qw8, https://github.com/eclipse/jetty.project/issues/9076	A-ECL-JETT-030523/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service -- although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize` which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory). **CVE ID : CVE-2023-26048**		
N/A	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the	https://github.com/eclipse/jetty.project/security/advisories/GHSA-p26g-97m4-6q7c, https://github.com/eclipse/jetty.project/pull/9352	A-ECL-JETT-030523/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote -- even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE ="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the	, https://github.com/eclipse/jetty.project/pull/9339	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-26049**		
Affected Version(s): 12.0.0					
N/A	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote -- even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE	https://github.com/eclipse/jetty.project/security/advisories/GHSA-p26g-97m4-6q7c, https://github.com/eclipse/jetty.project/pull/9352, https://github.com/eclipse/jetty.project/pull/9339	A-ECL-JETT-030523/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-26049**		
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.14					
Allocation of Resources	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. In	https://github.com/eclipse/jetty.proje	A-ECL-JETT-030523/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call `HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0` which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service -- although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize`	ct/pull/9345, https://github.com/eclipse/jetty.project/pull/9344, https://github.com/eclipse/jetty.project/security/advisories/GHSA-qw69-rqj8-6qw8, https://github.com/eclipse/jetty.project/issues/9076	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory). **CVE ID : CVE-2023-26048**		
N/A	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote -- even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because	https://github.com/eclipse/jetty.project/security/advisories/GHSA-p26g-97m4-6q7c, https://github.com/eclipse/jetty.project/pull/9352, https://github.com/eclipse/jetty.project/pull/9339	A-ECL-JETT-030523/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-26049**		
Affected Version(s): From (including) 11.0.0 Up to (excluding) 11.0.14					
Allocation of Resources Without Limits or Throttling	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. In affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call	https://github.com/eclipse/jetty.project/pull/9345, https://github.com/eclipse/jetty.project/pull/9344	A-ECL-JETT-030523/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0` which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service -- although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize` which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory).	, https://github.com/eclipse/jetty.project/security/advisories/GHSA-qw69-rqj8-6qw8, https://github.com/eclipse/jetty.project/issues/9076	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26048		
N/A	18-Apr-2023	5.3	Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote -- even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE ="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can	https://github.com/eclipse/jetty.project/security/advisories/GHSA-p26g-97m4-6q7c, https://github.com/eclipse/jetty.project/pull/9352, https://github.com/eclipse/jetty.project/pull/9339	A-ECL-JETT-030523/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-26049**		
Vendor: egostudiogroup					
Product: super_clean					
Affected Version(s): 1.1.5					
Uncontrolled Resource Consumption	20-Apr-2023	5.5	An issue found in Ego Studio SuperClean v.1.1.9 and v.1.1.5 allows an attacker to gain privileges cause a denial of service via the update_info field of the _default_.xml file. **CVE ID : CVE-2023-27652**	N/A	A-EGO-SUPE-030523/92
Affected Version(s): 1.1.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	20-Apr-2023	5.5	An issue found in Ego Studio SuperClean v.1.1.9 and v.1.1.5 allows an attacker to gain privileges cause a denial of service via the update_info field of the _default_.xml file. **CVE ID : CVE-2023-27652**	N/A	A-EGO-SUPE-030523/93
Vendor: electra-air					
Product: smart_kit_for_split_ac					
Affected Version(s): osk201					
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to load unauthorized FW. **CVE ID : CVE-2023-24503**	N/A	A-ELE-SMAR-030523/94
Vendor: electric_studio_client_login_project					
Product: electric_studio_client_login					
Affected Version(s): * Up to (including) 0.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in James Irving-Swift Electric Studio Client Login plugin <= 0.8.1 versions. **CVE ID : CVE-2023-27425**	N/A	A-ELE-ELEC-030523/95
Vendor: encode					
Product: starlette					
Affected Version(s): * Up to (excluding) 0.25.0					
Uncontrolled Resource	21-Apr-2023	7.5	There MultipartParser usage in Encode's Starlette python framework before	https://vulncheck.com/advisories/starlette-	A-ENC-STAR-030523/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			versions 0.25.0 allows an unauthenticated and remote attacker to specify any number of form fields or files which can cause excessive memory usage resulting in denial of service of the HTTP service. **CVE ID : CVE-2023-30798**	multipartparser-dos, https://github.com/encode/starlette/security/advisories/GHSA-74m5-2c7w-9w3x, https://github.com/encode/starlette/commit/8c74c2c8dba7030154f8af18e016136bea1938fa	
Vendor: faturamatik					
Product: bircard					
Affected Version(s): * Up to (excluding) 23.04.05					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Faturamatik Bircard allows SQL Injection.This issue affects Bircard: before 23.04.05. **CVE ID : CVE-2023-1873**	N/A	A-FAT-BIRC-030523/97
Vendor: freesoul_deactivate_plugins_-_plugin_manager_and_cleanup_project					
Product: freesoul_deactivate_plugins_-_plugin_manager_and_cleanup					
Affected Version(s): * Up to (including) 1.9.4.0					
Insecure Storage of	16-Apr-2023	7.5	Insecure Storage of Sensitive Information	N/A	A-FRE-FREE-030523/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			vulnerability in Jose Mortellaro Freesoul Deactivate Plugins – Plugin manager and cleanup plugin <= 1.9.4.0 versions. **CVE ID : CVE-2023-22687**		
Vendor: fullworksplugins					
Product: quick_paypal_payments					
Affected Version(s): * Up to (excluding) 5.7.26					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Paypal Payments plugin <= 5.7.25 versions. **CVE ID : CVE-2023-23889**	N/A	A-FUL-QUIC-030523/99
Vendor: gatsbyjs					
Product: gatsby					
Affected Version(s): * Up to (excluding) 4.25.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Apr-2023	4.3	gatsby-plugin-sharp is a plugin for the gatsby framework which exposes functions built on the Sharp image processing library. The gatsby-plugin-sharp plugin prior to versions 5.8.1 and 4.25.1 contains a path traversal vulnerability exposed when running the Gatsby develop server (`gatsby develop`). It should be noted that by default gatsby	https://github.com/gatsbyjs/gatsby/commit/dcf88ed01df2c26e0c93a41e1a2a840076d8247e, https://github.com/gatsbyjs/gatsby/commit/5f442081b227cc0879babb96858f970c4ce94c6b, https://githu	A-GAT-GATS-030523/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			develop is only accessible via the localhost 127.0.0.1, and one would need to intentionally expose the server to other interfaces to exploit this vulnerability by using server options such as --host 0.0.0.0, -H 0.0.0.0, or the GATSBY_HOST=0.0.0.0 environment variable. Attackers exploiting this vulnerability will have read access to all files within the scope of the server process. A patch has been introduced in gatsby-plugin-sharp@5.8.1 and gatsby-plugin-sharp@4.25.1 which mitigates the issue by ensuring that included paths remain within the project directory. As stated above, by default gatsby develop is only exposed to the localhost 127.0.0.1. For those using the develop server in the default configuration no risk is posed. If other ranges are required, preventing the develop server from being exposed to untrusted interfaces or IP address ranges would mitigate the risk from this vulnerability. Users	b.com/gatsbyjs/gatsby/security/advisories/GHSA-h2pm-378c-pcxx	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are non the less encouraged to upgrade to a safe version. **CVE ID : CVE-2023-30548**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.8.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Apr-2023	4.3	gatsby-plugin-sharp is a plugin for the gatsby framework which exposes functions built on the Sharp image processing library. The gatsby-plugin-sharp plugin prior to versions 5.8.1 and 4.25.1 contains a path traversal vulnerability exposed when running the Gatsby develop server (`gatsby develop`). It should be noted that by default gatsby develop is only accessible via the localhost 127.0.0.1, and one would need to intentionally expose the server to other interfaces to exploit this vulnerability by using server options such as --host 0.0.0.0, -H 0.0.0.0, or the GATSBY_HOST=0.0.0.0 environment variable. Attackers exploiting this vulnerability will have read access to all files within the scope of the server process. A patch has been	https://github.com/gatsbyjs/gatsby/commit/dcf88ed01df2c26e0c93a41e1a2a840076d8247e, https://github.com/gatsbyjs/gatsby/commit/5f442081b227cc0879babb96858f970c4ce94c6b, https://github.com/gatsbyjs/gatsby/security/advisories/GHSA-h2pm-378c-pcxx	A-GAT-GATS-030523/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduced in gatsby-plugin-sharp@5.8.1 and gatsby-plugin-sharp@4.25.1 which mitigates the issue by ensuring that included paths remain within the project directory. As stated above, by default gatsby develop is only exposed to the localhost 127.0.0.1. For those using the develop server in the default configuration no risk is posed. If other ranges are required, preventing the develop server from being exposed to untrusted interfaces or IP address ranges would mitigate the risk from this vulnerability. Users are non the less encouraged to upgrade to a safe version. **CVE ID : CVE-2023-30548**		
Vendor: gipsy_project					
Product: gipsy					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralization of Special Elements used in an OS Command	21-Apr-2023	9.8	Gipsy is a multi-purpose discord bot which aim to be as modular and user-friendly as possible. In versions prior to 1.3 users can run command on the host	https://github.com/Guniv ers/Gipsy/pull/24/commits/716818e967069f144aae66d51464b237c22	A-GIP-GIPS-030523/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			machine with sudoer permission. The `!ping` command when provided with an IP or hostname used to run a bash `ping <IP>` without verification that the IP or hostname was legitimate. This command was executed with root permissions and may lead to arbitrary command injection on the host server. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-30621**	b6cdf, https://github.com/Gunivers/Gipsy/pull/24, https://github.com/Curiosity-org/Gipsy/security/advisories/GHSA-6cw6-r8pg-j7wh	
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 112.0.5615.137					
Integer Overflow or Wraparound	19-Apr-2023	9.6	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2136**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	A-GOO-CHRO-030523/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2133**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	A-GOO-CHRO-030523/104
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2134**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	A-GOO-CHRO-030523/105
Out-of-bounds Write	19-Apr-2023	8.8	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2137**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	A-GOO-CHRO-030523/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Apr-2023	7.5	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2135**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	A-GOO-CHRO-030523/107
Vendor: google_maps_v3_shortcode_project					
Product: google_maps_v3_shortcode					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Google Maps v3 Shortcode plugin <= 1.2.1 versions. **CVE ID : CVE-2023-23827**	N/A	A-GOO-GOOG-030523/108
Vendor: i13websolution					
Product: responsive_filterable_portfolio					
Affected Version(s): * Up to (including) 1.0.19					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	The Responsive Filterable Portfolio plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.19 due to	N/A	A-I13-RESP-030523/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2119**		
Product: thumbnail_carousel_slider					
Affected Version(s): * Up to (including) 1.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	The Thumbnail carousel slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2120**	N/A	A-I13-THUM-030523/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: inisev					
Product: redirection					
Affected Version(s): * Up to (excluding) 1.1.5					
Cross-Site Request Forgery (CSRF)	17-Apr-2023	6.5	The Redirection WordPress plugin before 1.1.5 does not have CSRF checks in the uninstall action, which could allow attackers to make logged in admins delete all the redirections through a CSRF attack. **CVE ID : CVE-2023-1331**	N/A	A-INI-REDI-030523/111
Vendor: interactive_geo_maps_project					
Product: interactive_geo_maps					
Affected Version(s): * Up to (excluding) 1.5.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Carlos Moreira Interactive Geo Maps plugin <= 1.5.8 versions. **CVE ID : CVE-2023-23866**	N/A	A-INT-INTE-030523/112
Vendor: iteachyou					
Product: dreamer_cms					
Affected Version(s): 3.0.1					
Improper Neutralization of Input During Web Page Generation	18-Apr-2023	5.4	Dreamer CMS 3.0.1 is vulnerable to stored Cross Site Scripting (XSS). **CVE ID : CVE-2023-29774**	N/A	A-ITE-DREA-030523/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Vendor: jbootfly_project					
Product: jbootfly					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	Cross Site Scripting vulnerability found in Jbootfly allows attackers to obtain sensitive information via the username parameter. **CVE ID : CVE-2023-27092**	N/A	A-JBO-JBOO-030523/114
Vendor: json-content-importer					
Product: json_content_importer					
Affected Version(s): * Up to (excluding) 1.3.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Bernhard Kux JSON Content Importer plugin <= 1.3.15 versions. **CVE ID : CVE-2023-25485**	N/A	A-JSO-JSON-030523/115
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')	16-Apr-2023	9.8	A vulnerability has been found in SourceCodester Judging Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file	N/A	A-JUD-JUDG-030523/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			edit_contestant.php. The manipulation of the argument contestant_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226147. **CVE ID : CVE-2023-2108**		
Vendor: Juniper					
Product: appid_service_sigpack					
Affected Version(s): * Up to (excluding) 1.550.2-31					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and	https://supportportal.juniper.net/JSA70592	A-JUN-APPI-030523/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: jdpi-decoder_engine					
Affected Version(s): * Up to (excluding) 5.7.0-47					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos	https://supportportal.juniper.net/JSA70592	A-JUN-JDPI-030523/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: paragon_active_assurance					
Affected Version(s): * Up to (excluding) 4.1.2					
N/A	17-Apr-2023	7.2	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the timescaledb feature of Juniper Networks Paragon Active Assurance (PAA) (Formerly Netrounds) allows an attacker to bypass existing firewall rules and limitations used to restrict internal communcations. The Test Agents (TA) Appliance connects to the Control Center (CC) using OpenVPN. TA's are assigned an internal IP address in the 100.70.0.0/16 range. Firewall rules exists to limit communication from TA's to the CC to specific services only. OpenVPN is configured to not allow direct communication between Test Agents in the OpenVPN application itself, and routing is normally not enabled on the server running the CC	https://supportportal.juniper.net/JSA70595	A-JUN-PARA-030523/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application. The timescaledb feature is installed as an optional package on the Control Center. When the timescaledb container is started, this causes side-effects by bypassing the existing firewall rules and limitations for Test Agent communications. Note: This issue only affects customers hosting their own on-prem Control Center. The Paragon Active Assurance Software as a Service (SaaS) is not affected by this vulnerability since the timescaledb service is not enabled. This issue affects all on-prem versions of Juniper Networks Paragon Active Assurance prior to 4.1.2. **CVE ID : CVE-2023-28971**		
Vendor: link_juice_keeper_project					
Product: link_juice_keeper					
Affected Version(s): * Up to (excluding) 2.0.3					
Improper Neutralization of Input During Web Page Generation	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in George Pattihis Link Juice Keeper plugin <= 2.0.2 versions. **CVE ID : CVE-2023-25793**	N/A	A-LIN-LINK-030523/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Vendor: Linuxfoundation					
Product: kubewarden-controller					
Affected Version(s): * Up to (excluding) 1.6.0					
Improper Privilege Management	19-Apr-2023	8.8	An Improper Privilege Management vulnerability in SUSE kubewarden allows attackers to read arbitrary secrets if they get access to the ServiceAccount kubewarden-controller This issue affects: SUSE kubewarden kubewarden-controller versions prior to 1.6.0. **CVE ID : CVE-2023-22645**	https://bugzilla.suse.com/show_bug.cgi?id=1210218	A-LIN-KUBE-030523/121
Vendor: litextension					
Product: leurlrewrite					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2023	9.8	SQL injection vulnerability found in PrestaShopleurlrewrite v.1.0 and before allow a remote attacker to gain privileges via the Dispatcher::getController component. **CVE ID : CVE-2023-27844**	https://friends-of-presta.github.io/security-advisories/modules/2023/04/13/leurlrewrite.html	A-LIT-LEUR-030523/122
Vendor: m-files					
Product: m-files_server					
Affected Version(s): * Up to (excluding) 23.4.12528.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	20-Apr-2023	7.5	User-controlled operations could have allowed Denial of Service in M-Files Server before 23.4.12528.1 due to uncontrolled memory consumption. **CVE ID : CVE-2023-0383**	N/A	A-M-F-M-FI-030523/123
Uncontrolled Resource Consumption	20-Apr-2023	7.5	User-controlled operations could have allowed Denial of Service in M-Files Server before 23.4.12528.1 due to uncontrolled memory consumption for a scheduled job. **CVE ID : CVE-2023-0384**	N/A	A-M-F-M-FI-030523/124
Vendor: machothemes					
Product: regina_lite					
Affected Version(s): * Up to (including) 2.0.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	5.4	Auth (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Macho Themes Regina Lite theme <= 2.0.7 versions. **CVE ID : CVE-2023-27619**	N/A	A-MAC-REGI-030523/125
Vendor: mattermost					
Product: mattermost_server					
Affected Version(s): * Up to (excluding) 7.7.3					
Cleartext Transmission of Sensitive Information	17-Apr-2023	7.5	Mattermost fails to redact from audit logs the user password during user creation and the user password hash in other operations if the experimental audit logging configuration was enabled (ExperimentalAuditSettings section in config). **CVE ID : CVE-2023-1831**	https://mattermost.com/security-updates/	A-MAT-MATT-030523/126
Affected Version(s): 7.9.0					
Cleartext Transmission of Sensitive Information	17-Apr-2023	7.5	Mattermost fails to redact from audit logs the user password during user creation and the user password hash in other operations if the experimental audit logging configuration was enabled (ExperimentalAuditSe	https://mattermost.com/security-updates/	A-MAT-MATT-030523/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ttings section in config). **CVE ID : CVE-2023-1831**		
Affected Version(s): From (including) 7.8.0 Up to (excluding) 7.8.2					
Cleartext Transmission of Sensitive Information	17-Apr-2023	7.5	Mattermost fails to redact from audit logs the user password during user creation and the user password hash in other operations if the experimental audit logging configuration was enabled (ExperimentalAuditSettings section in config). **CVE ID : CVE-2023-1831**	https://mattermost.com/security-updates/	A-MAT-MATT-030523/128
Vendor: metagauss					
Product: themeflection_numbers					
Affected Version(s): * Up to (excluding) 2.0.1					
Cross-Site Request Forgery (CSRF)	17-Apr-2023	6.5	Themeflection Numbers WordPress plugin before 2.0.1 does not have authorisation and CSRF check in an AJAX action, and does not ensure that the options to be updated belong to the plugin. As a result, it could allow any authenticated users, such as subscriber, to update arbitrary blog options, such as	N/A	A-MET-THEM-030523/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabling registration and set the default role to administrator **CVE ID : CVE-2023-0889**		
Vendor: metaslider					
Product: slider\,_gallery\,_and_carousel					
Affected Version(s): * Up to (excluding) 3.29.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	6.1	The Slider, Gallery, and Carousel by MetaSlider WordPress plugin 3.29.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-1473**	N/A	A-MET-SLID-030523/130
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 1.3.4					
Exposure of Private Personal Information to an Unauthorized Actor	22-Apr-2023	6.5	Exposure of Private Personal Information to an Unauthorized Actor in GitHub repository microweber/microweber prior to 1.3.4. **CVE ID : CVE-2023-2239**	https://huntr.dev/bounties/edeff16b-fc71-4e26-8d2d-dfe7bb5e7868, https://github.com/microweber/microweber/commit/b0644cb3411b36b6ccc2ff7cdf7a	A-MIC-MICR-030523/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				f3fa49525baa	
Vendor: mindsdb					
Product: mindsdb					
Affected Version(s): * Up to (including) 23.1.5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Apr-2023	7.5	mindsdb is a Machine Learning platform to help developers build AI solutions. In affected versions an unsafe extraction is being performed using `tarfile.extractall()` from a remotely retrieved tarball. Which may lead to the writing of the extracted files to an unintended location. Sometimes, the vulnerability is called a TarSlip or a ZipSlip variant. An attacker may leverage this vulnerability to overwrite any local file which the server process has access to. There is no risk of file exposure with this vulnerability. This issue has been addressed in release `23.2.1.0 `. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-30620**	https://github.com/mindsdb/mindsdb/security/advisories/GHSA-2g5w-29q9-w6hx, https://github.com/mindsdb/mindsdb/commit/4419b0f0019c000db390b54d8b9d06e1d3670039	A-MIN-MIND-030523/132
Vendor: miniorange					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wordpress_social_login_and_register_\(discord\,_google\,_twitter\,_linkedin\)					
Affected Version(s): * Up to (excluding) 7.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in miniOrange WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin <= 7.5.14 versions. **CVE ID : CVE-2023-23710**	N/A	A-MIN-WORD-030523/133
Vendor: modoboa					
Product: modoboa					
Affected Version(s): * Up to (excluding) 2.1.0					
Weak Password Requirements	18-Apr-2023	9.8	Weak Password Requirements in GitHub repository modoboa/modoboa prior to 2.1.0. **CVE ID : CVE-2023-2160**	https://huntr.dev/bounties/54fb6d6a-6b39-45b6-b62a-930260ba484b, https://github.com/modoboa/modoboa/commit/130257c96a2392ada795785a91178e656e27015c	A-MOD-MODO-030523/134
Vendor: motor_racing_league_project					
Product: motor_racing_league					
Affected Version(s): * Up to (including) 1.9.9					
Improper Neutralization of Input During	23-Apr-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Ian Haycox Motor Racing	N/A	A-MOT-MOTO-030523/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			League plugin <= 1.9.9 versions. **CVE ID : CVE-2023-27614**		
Vendor: Nextcloud					
Product: nextcloud_files_automated_tagging					
Affected Version(s): 1.11.0					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/136
Affected Version(s): 1.12.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/137
Affected Version(s): 1.13.0					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99,	A-NEX-NEXT-030523/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	
Affected Version(s): 1.16.0					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**		
Affected Version(s): From (including) 1.14.0 Up to (excluding) 1.14.2					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**		
Affected Version(s): From (including) 1.15.0 Up to (excluding) 1.15.3					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/141
Product: nextcloud_server					
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.9.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/142
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.2.10.11					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99,	A-NEX-NEXT-030523/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.12.6					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.11					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**		
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.5					
N/A	17-Apr-2023	8.8	Nextcloud is a personal home server system. Depending on the set up tags and other workflows this issue can be used to limit access of others or being able to grant them access when there are system tag based files access control or files retention rules. It is recommended that the Nextcloud Server is upgraded to 24.0.11 or 25.0.5, the Nextcloud Enterprise Server to 21.0.9.11, 22.2.10.11, 23.0.12.6, 24.0.11 or 25.0.5, and the Nextcloud Files automated tagging app to 1.11.1, 1.12.1, 1.13.1, 1.14.2, 1.15.3 or 1.16.1. Users unable to upgrade should disable all workflow related apps. Users are advised to upgrade. **CVE ID : CVE-2023-30539**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-3m2f-v8x7-9w99, https://github.com/nextcloud/server/pull/37252, https://github.com/nextcloud/files_automatedtagging/pull/705	A-NEX-NEXT-030523/146
Product: talk					
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	4.3	Nextcloud Talk is a chat, video & audio call extension for Nextcloud. In affected versions a user that was added later to a conversation can use this information to get access to data that was deleted before they were added to the conversation. This issue has been patched in version 15.0.5 and it is recommended that users upgrad to 15.0.5. There are no known workarounds for this issue. **CVE ID : CVE-2023-30540**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-c9hr-cq65-9mjw, https://github.com/nextcloud/spreed/pull/8985	A-NEX-TALK-030523/147
Vendor: nuovo					
Product: spreadsheet-reader					
Affected Version(s): 0.5.11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Apr-2023	7.5	A Local File inclusion vulnerability in test.php in spreadsheet-reader 0.5.11 allows remote attackers to include arbitrary files via the File parameter. **CVE ID : CVE-2023-29887**	N/A	A-NUO-SPRE-030523/148
Vendor: nuxtlabs					
Product: nuxt					
Affected Version(s): * Up to (excluding) 1.6.2					
Use of Hard-	18-Apr-2023	9.8	Use of Hard-coded Credentials in GitHub repository	https://github.com/nuxtlabs/github-	A-NUX-NUXT-030523/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			nuxtlabs/github-module prior to 1.6.2. **CVE ID : CVE-2023-2138**	module/commit/5490c43f729eee60f07920bf88c0aabdc1398b6e, https://huntr.dev/bounties/65096ef9-eafc-49da-b49a-5b88c0203ca6	
Vendor: online_eyewear_shop_project					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. This affects an unknown part of the file /admin/orders/update_status.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-227229 was assigned to this vulnerability. **CVE ID : CVE-2023-2244**	N/A	A-ONL-ONLI-030523/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: online_jewelry_shop_project					
Product: online_jewelry_shop					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-2023	5.4	A stored cross-site scripting (XSS) vulnerability in /index.php?page=category_list of Online Jewelry Shop v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Category Name parameter. **CVE ID : CVE-2023-27776**	N/A	A-ONL-ONLI-030523/151
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-2023	5.4	Cross-site scripting (XSS) vulnerability was discovered in Online Jewelry Shop v1.0 that allows attackers to execute arbitrary script via a crafted URL. **CVE ID : CVE-2023-27777**	N/A	A-ONL-ONLI-030523/152
Vendor: online_pizza_ordering_system_project					
Product: online_pizza_ordering_system					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	23-Apr-2023	9.8	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file admin/ajax.php?actio	N/A	A-ONL-ONLI-030523/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n=save_settings. The manipulation of the argument img leads to unrestricted upload. 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-227236. **CVE ID : CVE-2023-2246**		
Vendor: online_thesis_archiving_system_project					
Product: online_thesis_archiving_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/departments/view_department.php. 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 identifier VDB-226265 was assigned to this vulnerability. **CVE ID : CVE-2023-2144**	N/A	A-ONL-ONLI-030523/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0. It has been classified as critical. Affected is an unknown function of the file projects_per_curriculum.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226266 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2145**	N/A	A-ONL-ONLI-030523/155
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file classes/Master.php. The manipulation of the argument name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of	N/A	A-ONL-ONLI-030523/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability is VDB-226267. **CVE ID : CVE-2023-2146**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability was found in Campcodes Online Thesis Archiving System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/students/view_details.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226268. **CVE ID : CVE-2023-2147**	N/A	A-ONL-ONLI-030523/157
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability classified as critical has been found in Campcodes Online Thesis Archiving System 1.0. This affects an unknown part of the file /admin/curriculum/view_curriculum.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The	N/A	A-ONL-ONLI-030523/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The identifier VDB-226269 was assigned to this vulnerability. **CVE ID : CVE-2023-2148**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability classified as critical was found in Campcodes Online Thesis Archiving System 1.0. This vulnerability affects unknown code of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-226270 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2149**	N/A	A-ONL-ONLI-030523/159
Vendor: openzeppelin					
Product: contracts					
Affected Version(s): From (including) 3.2.0 Up to (excluding) 4.8.3					
Interpretation Conflict	17-Apr-2023	5.3	OpenZeppelin Contracts is a library for secure smart contract development. A function in the implementation contract may be inaccessible if its	https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-mx2q-35m2-	A-OPE-CONT-030523/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			selector clashes with one of the proxy's own selectors. Specifically, if the clashing function has a different signature with incompatible ABI encoding, the proxy could revert while attempting to decode the arguments from calldata. The probability of an accidental clash is negligible, but one could be caused deliberately and could cause a reduction in availability. The issue has been fixed in version 4.8.3. As a workaround if a function appears to be inaccessible for this reason, it may be possible to craft the calldata such that ABI decoding does not fail at the proxy and the function is properly proxied through. **CVE ID : CVE-2023-30541**	x2rh, https://github.com/OpenZeppelin/openzeppelin-contracts/pull/4154	
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.8.3					
N/A	16-Apr-2023	8.8	OpenZeppelin Contracts is a library for secure smart contract development. The proposal creation entrypoint (`propose`) in `GovernorCompatibilityBravo` allows the	https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-93hq-5wgc-jc82	A-OPE-CONT-030523/161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creation of proposals with a `signatures` array shorter than the `calldatas` array. This causes the additional elements of the latter to be ignored, and if the proposal succeeds the corresponding actions would eventually execute without any calldata. The `ProposalCreated` event correctly represents what will eventually execute, but the proposal parameters as queried through `getActions` appear to respect the original intended calldata. This issue has been patched in 4.8.3. As a workaround, ensure that all proposals that pass through governance have equal length `signatures` and `calldatas` parameters. **CVE ID : CVE-2023-30542**		
Product: contracts_upgradeable					
Affected Version(s): From (including) 3.2.0 Up to (excluding) 4.8.3					
Interpretation Conflict	17-Apr-2023	5.3	OpenZeppelin Contracts is a library for secure smart contract development. A function in the implementation contract may be inaccessible if its selector clashes with	https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-mx2q-35m2-x2rh,	A-OPE-CONT-030523/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one of the proxy's own selectors. Specifically, if the clashing function has a different signature with incompatible ABI encoding, the proxy could revert while attempting to decode the arguments from calldata. The probability of an accidental clash is negligible, but one could be caused deliberately and could cause a reduction in availability. The issue has been fixed in version 4.8.3. As a workaround if a function appears to be inaccessible for this reason, it may be possible to craft the calldata such that ABI decoding does not fail at the proxy and the function is properly proxied through. **CVE ID : CVE-2023-30541**	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/4154	
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.8.3					
N/A	16-Apr-2023	8.8	OpenZeppelin Contracts is a library for secure smart contract development. The proposal creation entrypoint (`propose`) in `GovernorCompatibilityBravo` allows the creation of proposals	https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-93hq-5wgc-jc82	A-OPE-CONT-030523/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a `signatures` array shorter than the `calldatas` array. This causes the additional elements of the latter to be ignored, and if the proposal succeeds the corresponding actions would eventually execute without any calldata. The `ProposalCreated` event correctly represents what will eventually execute, but the proposal parameters as queried through `getActions` appear to respect the original intended calldata. This issue has been patched in 4.8.3. As a workaround, ensure that all proposals that pass through governance have equal length `signatures` and `calldatas` parameters. **CVE ID : CVE-2023-30542**		
Vendor: Oracle					
Product: application_object_library					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.11					
N/A	18-Apr-2023	6.5	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: GUI). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-APPL-030523/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.2.3-12.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data as well as unauthorized read access to a subset of Oracle Application Object Library accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Object Library. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21978**		
Product: banking_payments					
Affected Version(s): 14.5					
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Book/Internal Transfer). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21915**		
Affected Version(s): 14.6					
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Book/Internal Transfer). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Banking Payments accessible data as well as unauthorized read	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle Banking Payments accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21915**		
Affected Version(s): 14.7					
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Book/Internal Transfer). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Banking Payments accessible data as well as unauthorized read access to a subset of Oracle Banking Payments accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21915**		
Product: banking_virtual_account_management					
Affected Version(s): 14.5					
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: Routing Hub). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21905**		
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: SMS Module). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21906**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7.	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21907		
N/A	18-Apr-2023	6	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H). **CVE ID : CVE-2023-21908**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Internal Tfr Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-21903**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-21904**		
Affected Version(s): 14.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: Routing Hub). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21905**		
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: SMS Module). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21906**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H). **CVE ID : CVE-2023-21907**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H). **CVE ID : CVE-2023-21908**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Banking Virtual	https://www.oracle.com	A-ORA-BANK-030523/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Account Management product of Oracle Financial Services Applications (component: OBVAM Internal Tfr Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management.	/security-alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-21903**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-21904**		
Affected Version(s): 14.7					
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: Routing Hub). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management.	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21905**		
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: SMS Module). Supported versions that are affected are 14.5, 14.6 and 14.7. Easily exploitable	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Virtual Account Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21906**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H). **CVE ID : CVE-2023-21907**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 6.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:H). **CVE ID : CVE-2023-21908**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Internal Tfr Domain). Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-21903**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Banking Virtual Account Management product of Oracle Financial Services Applications (component: OBVAM Trn Journal Domain).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BANK-030523/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 14.5, 14.6 and 14.7. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Virtual Account Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Virtual Account Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Banking Virtual Account Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Virtual Account Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:H/UI:R/S:U/C:H/I:L/A:L). **CVE ID : CVE-2023-21904**		
Product: bi_publisher					
Affected Version(s): 12.2.1.4.0					
N/A	18-Apr-2023	4.3	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21941**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BI_P-030523/186
Affected Version(s): 6.4.0.0.0					
N/A	18-Apr-2023	5.7	Vulnerability in the Oracle BI Publisher product of Oracle	https://www.oracle.com/security-	A-ORA-BI_P-030523/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Analytics (component: Security). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21970**	alerts/cpuapr2023.html	
N/A	18-Apr-2023	4.3	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BI_P-030523/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21941**		
Product: business_intelligence					
Affected Version(s): 12.2.1.4.0					
N/A	18-Apr-2023	6.5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web General). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition.	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BUSI-030523/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21910**		
Affected Version(s): 6.4.0.0.0					
N/A	18-Apr-2023	6.5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web General). Supported versions that are affected are 6.4.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BUSI-030523/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21910**		
N/A	18-Apr-2023	5.7	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BUSI-030523/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21952**		
N/A	18-Apr-2023	5.7	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-BUSI-030523/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21965**		
Product: clinical_remote_data_capture					
Affected Version(s): 5.4.0.2					
N/A	18-Apr-2023	6.5	Vulnerability in the Oracle Clinical Remote Data Capture product of Oracle Health Sciences Applications (component: Forms). The supported version that is affected is 5.4.0.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Clinical Remote Data Capture. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Clinical Remote Data Capture accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-CLIN-030523/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21993**		
Product: database					
Affected Version(s): 19c					
N/A	18-Apr-2023	6.8	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows low privileged attacker having User Account privilege with network access via TLS to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data as well as unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-DATA-030523/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21934**		
Affected Version(s): 21c					
N/A	18-Apr-2023	6.8	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Difficult to exploit vulnerability allows low privileged attacker having User Account privilege with network access via TLS to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data as well as unauthorized access to critical data or complete access to all Java VM accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21934**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-DATA-030523/195
Product: database_recovery_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 19c					
N/A	18-Apr-2023	6.8	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having Local SYSDBA privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. While the vulnerability is in Oracle Database Recovery Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Database Recovery Manager. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-DATA-030523/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21918		
Affected Version(s): 21c					
N/A	18-Apr-2023	6.8	Vulnerability in the Oracle Database Recovery Manager component of Oracle Database Server. Supported versions that are affected are 19c and 21c. Easily exploitable vulnerability allows high privileged attacker having Local SYSDBA privilege with network access via Oracle Net to compromise Oracle Database Recovery Manager. While the vulnerability is in Oracle Database Recovery Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Database Recovery Manager. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-DATA-030523/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:H/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2023-21918**		
Product: essbase					
Affected Version(s): 21.4					
N/A	18-Apr-2023	5.3	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21942**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-ESSB-030523/198
N/A	18-Apr-2023	5.3	Vulnerability in Oracle Essbase (component:	https://www.oracle.com	A-ORA-ESSB-030523/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21943**	/security-alerts/cpuapr2023.html	
N/A	18-Apr-2023	5.3	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-ESSB-030523/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Essbase. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Essbase accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21944**		
Product: financial_services_behavior_detection_platform					
Affected Version(s): 8.0.8.1					
N/A	18-Apr-2023	4.3	Vulnerability in the Oracle Financial Services Behavior Detection Platform product of Oracle Financial Services Applications (component: Application). The supported version that is affected is 8.0.8.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-FINA-030523/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Financial Services Behavior Detection Platform. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Behavior Detection Platform accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21902**		
Product: graalvm					
Affected Version(s): 20.3.8					
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 20.3.9					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments,	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.7	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle GraalVM Enterprise Edition executes to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 5.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L). **CVE ID : CVE-2023-21986**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 21.3.4					
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
Affected Version(s): 21.3.5					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	5.7	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle GraalVM Enterprise Edition executes to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM Enterprise Edition.	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 5.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L). **CVE ID : CVE-2023-21986**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21937		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Affected Version(s): 22.3.0					
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
Affected Version(s): 22.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21954		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.7	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Native Image). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle GraalVM Enterprise Edition executes to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.1 Base Score 5.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L). **CVE ID : CVE-2023-21986**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21939		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-GRAA-030523/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Product: health_sciences_inform					
Affected Version(s): * Up to (excluding) 6.3.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	8.3	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L). **CVE ID : CVE-2023-21923**		
N/A	18-Apr-2023	6.8	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21922**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Health Sciences InForm, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21924**		
N/A	18-Apr-2023	5.5	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Health Sciences InForm executes to compromise Oracle Health Sciences	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InForm. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21926**		
N/A	18-Apr-2023	5.4	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized update, insert or delete access to some of Oracle Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21921**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized ability to cause a	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21925**		
Affected Version(s): 7.0.0.0					
N/A	18-Apr-2023	8.3	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			complete access to all Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L). **CVE ID : CVE-2023-21923**		
N/A	18-Apr-2023	6.8	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21922**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person other than the attacker and while the vulnerability is in Oracle Health Sciences InForm, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-21924**		
N/A	18-Apr-2023	5.5	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Health Sciences InForm executes to compromise Oracle Health Sciences InForm. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21926**		
N/A	18-Apr-2023	5.4	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences InForm accessible data as well as unauthorized read access to a subset of Oracle Health Sciences InForm accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21921**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HEAL-030523/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21925**		
Product: hospitality_opera_5_property_services					
Affected Version(s): 5.6					
N/A	18-Apr-2023	7.2	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: OXI). The supported version that is affected is 5.6. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-HOSP-030523/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hospitality OPERA 5 Property Services. While the vulnerability is in Oracle Hospitality OPERA 5 Property Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality OPERA 5 Property Services accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L). **CVE ID : CVE-2023-21932**		
Product: iprocurement					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Apr-2023	5.4	Vulnerability in the Oracle iProcurement product of Oracle E-Business Suite (component: E-Content Manager Catalog). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iProcurement, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle iProcurement accessible data as well as unauthorized read access to a subset of Oracle iProcurement accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-IPRO-030523/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21973**		
Product: ireceivables					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Apr-2023	4.3	Vulnerability in the Oracle iReceivables product of Oracle E-Business Suite (component: Attachments). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iReceivables. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle iReceivables accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21959**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-IREC-030523/240
Product: jdk					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.8.0					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments,	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-ORA-JDK-030523/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update,	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Affected Version(s): 11.0.18					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Affected Version(s): 17.0.6					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21930		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-ORA-JDK-030523/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Affected Version(s): 20					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21939		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JDK-030523/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-	A-ORA-JDK-030523/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Product: jd_edwards_enterpriseone_tools					
Affected Version(s): * Up to (excluding) 9.2.7.3					
N/A	18-Apr-2023	5.4	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are Prior to 9.2.7.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JD_E-030523/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21936**		
N/A	18-Apr-2023	4.3	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Interoperability SEC). Supported versions that are affected are Prior to 9.2.7.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JD_E-030523/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21927**		
Product: jre					
Affected Version(s): 1.8.0					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21930		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-ORA-JRE-030523/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Affected Version(s): 11.0.18					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-	A-ORA-JRE-030523/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Affected Version(s): 17.0.6					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21954**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of	https://www.oracle.com/security-	A-ORA-JRE-030523/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21968		
Affected Version(s): 20					
N/A	18-Apr-2023	7.4	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2023-21930**		
N/A	18-Apr-2023	5.9	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21967**		
N/A	18-Apr-2023	5.3	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21939**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21937**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-	A-ORA-JRE-030523/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21938**		
N/A	18-Apr-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-JRE-030523/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21968**		
Product: mysql					
Affected Version(s): * Up to (including) 8.0.32					
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21977**		
Affected Version(s): From (including) 5.0.0 Up to (including) 5.7.41					
N/A	18-Apr-2023	7.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21980**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.32					
N/A	18-Apr-2023	7.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21980**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21972**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21976**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/301
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21982**		
Product: mysql_connectors					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.32					
N/A	18-Apr-2023	5.3	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors as well as unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:H). **CVE ID : CVE-2023-21971**		
Product: mysql_server					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.32					
N/A	18-Apr-2023	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21946**		
N/A	18-Apr-2023	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2023-21929**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21911		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21919**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/307
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21920**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21933**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21935		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21945**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/311
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.32 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21953**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21955**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21962		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21966**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/315
N/A	18-Apr-2023	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21940**		
N/A	18-Apr-2023	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.32 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21947**		
Affected Version(s): From (including) 5.7.0 Up to (including) 5.7.40					
N/A	18-Apr-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.40 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21963		
Affected Version(s): From (including) 5.7.0 Up to (including) 5.7.41					
N/A	18-Apr-2023	7.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.41 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21912**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/319
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.30					
N/A	18-Apr-2023	7.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 5.7.41 and prior and 8.0.30 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21912**		
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.30 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21917**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.31					
N/A	18-Apr-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21913**		
N/A	18-Apr-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 5.7.40 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-21963**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-MYSQ-030523/323
Product: peoplesoft_enterprise_human_capital_management_human_resources					
Affected Version(s): 9.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	5.4	Vulnerability in the PeopleSoft Enterprise HCM Human Resources product of Oracle PeopleSoft (component: Administer Workforce). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Human Resources. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Human Resources accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HCM Human Resources accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21992**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: peoplesoft_enterprise_peopletools					
Affected Version(s): 8.58					
N/A	18-Apr-2023	5.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Web Server). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21916**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/325
N/A	18-Apr-2023	4.9	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21981**		
Affected Version(s): 8.59					
N/A	18-Apr-2023	5.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Web Server). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21916**		
N/A	18-Apr-2023	4.9	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21981**		
Affected Version(s): 8.60					
N/A	18-Apr-2023	5.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Web Server). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21916**		
N/A	18-Apr-2023	4.9	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Elastic Search). Supported versions that are affected are 8.58, 8.59 and 8.60. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21981**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-PEOP-030523/330
Product: siebel_crm					
Affected Version(s): * Up to (including) 23.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	6.5	Vulnerability in the Siebel CRM product of Oracle Siebel CRM (component: UI Framework). Supported versions that are affected are 23.3 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21909**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-SIEB-030523/331
Product: sql_developer					
Affected Version(s): * Up to (excluding) 23.1.0					
N/A	18-Apr-2023	6.7	Vulnerability in Oracle SQL Developer (component: Installation). Supported versions that are affected are Prior to 23.1.0. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-SQL_-030523/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			high privileged attacker with logon to the infrastructure where Oracle SQL Developer executes to compromise Oracle SQL Developer. Successful attacks of this vulnerability can result in takeover of Oracle SQL Developer. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21969**		
Product: user_management					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Apr-2023	4.3	Vulnerability in the Oracle User Management product of Oracle E-Business Suite (component: Proxy User Delegation). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle User Management. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-USER-030523/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle User Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-21997**		
Product: vm_virtualbox					
Affected Version(s): * Up to (excluding) 6.1.44					
N/A	18-Apr-2023	8.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21990**		
N/A	18-Apr-2023	7.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21987**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2023-21989**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22002		
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21998**		
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22000**		
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22001**		
N/A	18-Apr-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2023-21988**		
N/A	18-Apr-2023	3.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21999**		
N/A	18-Apr-2023	3.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21991		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.8					
N/A	18-Apr-2023	8.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21990**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	7.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21987**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/345
N/A	18-Apr-2023	6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2023-21989**		
N/A	18-Apr-2023	6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2023-22002**		
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21998**		
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization	https://www.oracle.com/security-	A-ORA-VM_V-030523/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22000**	alerts/cpuapr2023.html	
N/A	18-Apr-2023	4.6	Vulnerability in the Oracle VM VirtualBox	https://www.oracle.com	A-ORA-VM_V-030523/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22001**	/security-alerts/cpuapr2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	3.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2023-21988**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/351
N/A	18-Apr-2023	3.6	Vulnerability in the Oracle VM VirtualBox product of Oracle	https://www.oracle.com/security-	A-ORA-VM_V-030523/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.44 and Prior to 7.0.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-21999**	alerts/cpuapr2023.html	
N/A	18-Apr-2023	3.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-VM_V-030523/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Prior to 6.1.44 and Prior to 7.0.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2023-21991**		
Product: weblogic_server					
Affected Version(s): 12.2.1.4.0					
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21931**		
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server.	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21964**		
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21979**		
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21996**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-21956**		
N/A	18-Apr-2023	5.6	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 5.6 (Confidentiality, Integrity and	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2023-21960**		
Affected Version(s): 12.2.1.3.0					
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21931**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21964**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/361
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21979**		
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21996**		
N/A	18-Apr-2023	5.6	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2023-21960**		
Affected Version(s): 14.1.1.0.0					
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21931**		
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21964		
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21979**	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/367
N/A	18-Apr-2023	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21996**		
N/A	18-Apr-2023	6.1	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to	https://www.oracle.com/security-alerts/cpuapr2023.html	A-ORA-WEBL-030523/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L /PR:N/UI:R/S:C/C:L/I: L/A:N). **CVE ID : CVE-2023-21956**		
Vendor: Phoenixcontact					
Product: energy_axc_pu					
Affected Version(s): From (including) 01.00.00.00 Up to (including) 04.15.00.00					
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an authenticated restricted user of the	N/A	A-PHO-ENER-030523/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**		
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1875**	https://github.com/thorsten/phpmyfaq/commit/dcf7dd43a3412aa951d7087b86a8b917fae2133a, https://huntr.dev/bounties/39715aaf-e798-4c60-97c4-45f4f2cd5c61	A-PHP-PHPM-030523/371
Vendor: php_execution_project					
Product: php_execution					
Affected Version(s): * Up to (including) 1.0.0					
Cross-Site Request Forgery (CSRF)	23-Apr-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Nicolas Zeh PHP Execution plugin <= 1.0.0 versions.	N/A	A-PHP-PHP_-030523/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23879		
Vendor: Piwigo					
Product: piwigo					
Affected Version(s): * Up to (including) 13.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Apr-2023	8.8	SQL injection vulnerability found in Piwigo v.13.5.0 and before allows a remote attacker to execute arbitrary code via the filter_user_id parameter to the admin.php?page=history&filter_image_id=&filter_user_id endpoint. **CVE ID : CVE-2023-26876**	N/A	A-PIW-PIWI-030523/373
Vendor: podlove					
Product: podlove_subscribe_button					
Affected Version(s): * Up to (excluding) 1.3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Podlove Podlove Subscribe button plugin <= 1.3.7 versions. **CVE ID : CVE-2023-25479**	N/A	A-POD-PODL-030523/374
Vendor: podofo_project					
Product: podofo					
Affected Version(s): 0.10.0					
Heap-based Buffer Overflow	22-Apr-2023	7.8	A vulnerability, which was classified as critical, was found in PoDoFo 0.10.0. Affected is the function	https://github.com/podofo/podofo/commit/535a786f124b739e3c857529c	A-POD-PODO-030523/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			readXRefStreamEntry of the file PdfXRefStreamParserObject.cpp. The manipulation leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The name of the patch is 535a786f124b739e3c857529cecc29e4eeb79778. It is recommended to apply a patch to fix this issue. VDB-227226 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2241**	ecc29e4eeb79778	
Vendor: portfolio_slideshow_project					
Product: portfolio_slideshow					
Affected Version(s): * Up to (including) 1.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in George Gecewicz Portfolio Slideshow plugin <= 1.13.0 versions. **CVE ID : CVE-2023-23717**	N/A	A-POR-PORT-030523/376
Vendor: powerjob					
Product: powerjob					
Affected Version(s): 4.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Apr-2023	9.8	PowerJob V4.3.1 is vulnerable to Incorrect Access Control that allows for remote code execution. **CVE ID : CVE-2023-29924**	N/A	A-POW-POWE-030523/377
N/A	19-Apr-2023	5.3	PowerJob V4.3.1 is vulnerable to Incorrect Access Control via the create user/save interface. **CVE ID : CVE-2023-29922**	N/A	A-POW-POWE-030523/378
Incorrect Default Permissions	19-Apr-2023	5.3	PowerJob V4.3.1 is vulnerable to Insecure Permissions. via the list job interface. **CVE ID : CVE-2023-29923**	N/A	A-POW-POWE-030523/379
Affected Version(s): 4.3.2					
N/A	20-Apr-2023	9.8	PowerJob V4.3.2 has unauthorized interface that causes remote code execution. **CVE ID : CVE-2023-29926**	N/A	A-POW-POWE-030523/380
Vendor: pricing_tables_for_wpbakery_page_builder_project					
Product: pricing_tables_for_wpbakery_page_builder					
Affected Version(s): * Up to (excluding) 3.0					
Improper Limitation of a Pathname to a Restricted Directory	17-Apr-2023	6.5	The Pricing Tables For WPBakery Page Builder (formerly Visual Composer) WordPress plugin before 3.0 does not validate some shortcode attributes	N/A	A-PRI-PRIC-030523/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			before using them to generate paths passed to include function/s, allowing any authenticated users such as subscriber to perform LFI attacks **CVE ID : CVE-2023-1274**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	5.4	The Pricing Tables For WPBakery Page Builder (formerly Visual Composer) WordPress plugin before 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-2023-0367**	N/A	A-PRI-PRIC-030523/382
Vendor: purchase_order_management_system_project					
Product: purchase_order_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	17-Apr-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Purchase Order Management System 1.0. Affected is an unknown function of the file /admin/suppliers/vie	N/A	A-PUR-PURC-030523/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			w_details.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-226206 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2130**		
Vendor: Python					
Product: python					
Affected Version(s): * Up to (including) 2.7.18					
Improper Input Validation	19-Apr-2023	5.3	The e-mail module of Python 0 - 2.7.18, 3.x - 3.11 incorrectly parses e-mail addresses which contain a special character. This vulnerability allows attackers to send messages from e-ail addresses that would otherwise be rejected. **CVE ID : CVE-2023-27043**	N/A	A-PYT-PYTH-030523/384
Affected Version(s): From (including) 3.0 Up to (including) 3.11					
Improper Input Validation	19-Apr-2023	5.3	The e-mail module of Python 0 - 2.7.18, 3.x - 3.11 incorrectly parses e-mail addresses which contain a special character. This	N/A	A-PYT-PYTH-030523/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to send messages from e-ail addresses that would otherwise be rejected. **CVE ID : CVE-2023-27043**		
Vendor: qualys					
Product: cloud_agent					
Affected Version(s): From (including) 2.5.1-75 Up to (excluding) 3.7					
Untrusted Search Path	18-Apr-2023	7	Qualys Cloud Agent for macOS (versions 2.5.1-75 before 3.7) installer allows a local escalation of privilege bounded only to the time of installation and only on older macOSX (macOS 10.15 and older) versions. Attackers may exploit incorrect file permissions to give them ROOT command execution privileges on the host. During the install of the PKG, a step in the process involves extracting the package and copying files to several directories. Attackers may gain writable access to files during the install of PKG when extraction of the package and	https://qualys.com/security-advisories	A-QUA-CLOU-030523/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			copying files to several directories, enabling a local escalation of privilege. **CVE ID : CVE-2023-28143**		
Affected Version(s): From (including) 3.1.3.34 Up to (excluding) 4.5.3.1					
Uncontrolled Search Path Element	18-Apr-2023	7	An Executable Hijacking condition exists in the Qualys Cloud Agent for Windows platform in versions before 4.5.3.1. Attackers may load a malicious copy of a Dependency Link Library (DLL) via a local attack vector instead of the DLL that the application was expecting, when processes are running with escalated privileges. This vulnerability	https://www.qualys.com/security-advisories/	A-QUA-CLOU-030523/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is bounded only to the time of uninstallation and can only be exploited locally. At the time of this disclosure, versions before 4.0 are classified as End of Life. **CVE ID : CVE-2023-28140**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-Apr-2023	7	A Race Condition exists in the Qualys Cloud Agent for Windows platform in versions from 3.1.3.34 and before 4.5.3.1. This allows attackers to escalate privileges limited on the local machine during uninstallation of the Qualys Cloud Agent for Windows. Attackers may gain SYSTEM level privileges on that asset to run arbitrary commands. At the time of this disclosure, versions before 4.0 are classified as End of Life.	https://www.qualys.com/security-advisories/	A-QUA-CLOU-030523/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28142		
Affected Version(s): From (including) 3.1.3.34 Up to (excluding) 4.8.0.31					
N/A	18-Apr-2023	6.3	An NTFS Junction condition exists in the Qualys Cloud Agent for Windows platform in versions before 4.8.0.31. Attackers may write files to arbitrary locations via a local attack vector. This allows attackers to assume the privileges of the process, and they may delete or otherwise on unauthorized files, allowing for the potential modification or deletion of sensitive files limited only to that specific directory/file object. This vulnerability is bounded to the time of installation/uninstalla	https://www.qualys.com/security-advisories/	A-QUA-CLOU-030523/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tion and can only be exploited locally. At the time of this disclosure, versions before 4.0 are classified as End of Life. **CVE ID : CVE-2023-28141**		
Vendor: rarathemes					
Product: vryasage_marketing_performance					
Affected Version(s): * Up to (including) 2.0.0					
Improper Neutralization of Input	23-Apr-2023	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in VryaSage Marketing	N/A	A-RAR-VRYA-030523/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Performance plugin <= 2.0.0 versions. **CVE ID : CVE-2023-24404**		
Vendor: redis					
Product: redis					
Affected Version(s): * Up to (excluding) 6.0.19					
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	https://github.com/redis/redis/commit/bc7fe41e5857a0854d524e2a63a028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-hjv8-vjf6-wcr6, https://github.com/redis/redis/pull/11149	A-RED-REDI-030523/391
Affected Version(s): From (including) 6.2.0 Up to (excluding) 6.2.12					
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11,	https://github.com/redis/redis/commit/bc7fe41e5857a0854d524e2a63a028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-	A-RED-REDI-030523/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	hjv8-vjf6-wcr6, https://github.com/redis/redis/pull/11149	
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.11					
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	https://github.com/redis/redis/commit/bc7fe41e5857a0854d524e2a63a028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-hjv8-vjf6-wcr6, https://github.com/redis/redis/pull/11149	A-RED-REDI-030523/393
Vendor: roxy-wi					
Product: roxy-wi					
Affected Version(s): * Up to (including) 6.3.9.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Apr-2023	6.5	hap-wi/roxy-wi is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. A Path Traversal vulnerability was found in the current version of Roxy-WI (6.3.9.0 at the moment	https://github.com/hap-wi/roxy-wi/security/advisories/GHSA-7qqj-xhvr-46fv	A-ROX-ROXY-030523/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of writing this report). The vulnerability can be exploited via an HTTP request to /app/options.py and the config_file_name parameter. Successful exploitation of this vulnerability could allow an attacker with user level privileges to obtain the content of arbitrary files on the file server within the scope of what the server process has access to. The root-cause of the vulnerability lies in the get_config function of the /app/modules/config /config.py file, which only checks for relative path traversal, but still allows to read files from absolute locations passed via the config_file_name parameter. **CVE ID : CVE-2023-29004**		
Vendor: Schneider-electric					
Product: apc_easy_ups_online_monitoring_software					
Affected Version(s): * Up to (including) 2.5-ga-01-22320					
Missing Authentication for Critical Function	18-Apr-2023	9.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-	A-SCH-APC_-030523/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface. **CVE ID : CVE-2023-29411**	04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	9.8	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface. **CVE ID : CVE-2023-29412**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	A-SCH-APC_-030523/396
Missing Authentication for	18-Apr-2023	7.5		https://download.schneider-	A-SCH-APC_-030523/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service. **CVE ID : CVE-2023-29413**	electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	
Product: easy_ups_online_monitoring_software					
Affected Version(s): * Up to (including) 2.5-gs-01-22320					
Missing Authentication for Critical Function	18-Apr-2023	9.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	A-SCH-EASY-030523/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29411		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	9.8	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface. **CVE ID : CVE-2023-29412**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	A-SCH-EASY-030523/399
Missing Authentication for Critical Function	18-Apr-2023	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	A-SCH-EASY-030523/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29413		
Product: struxureware_data_center_expert					
Affected Version(s): * Up to (including) 7.9.2					
Improper Control of Generation of Code ('Code Injection')	18-Apr-2023	9.8	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that allows for remote code execution when using a parameter of the DCE network settings endpoint.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25549**		
Improper Control of Generation of Code ('Code Injection')	18-Apr-2023	9.8	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that allows remote code execution via the “hostname” parameter when maliciously crafted hostname syntax is entered.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25550**		
Incorrect Authorization	18-Apr-2023	8.8	A CWE-863: Incorrect Authorization vulnerability exists that could allow remote code execution on upload and install packages when a hacker is using a low privileged user account. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25547**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/403
Missing Authorization	18-Apr-2023	8.1	A CWE-862: Missing Authorization vulnerability exists that could allow	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDoc	A-SCH-STRU-030523/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			viewing of unauthorized content, changes or deleting of content, or performing unauthorized functions when tampering the Device File Transfer settings on DCE endpoints. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25552**	Type=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	8.1		https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could allow a user that knows the credentials to execute unprivileged shell commands on the appliance over SSH. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25555		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	7.8	A CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that allows a local privilege escalation on the appliance when a maliciously crafted Operating System command is entered on the device. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25554**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/406
Incorrect Authorization	18-Apr-2023	6.5	A CWE-863: Incorrect Authorization vulnerability exists	https://download.schneider-electric.com/	A-SCH-STRU-030523/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could allow access to device credentials on specific DCE endpoints not being properly secured when a hacker is using a low privileged user. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25548**	files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists on a DCE file upload endpoint when	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tampering with parameters over HTTP. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25551**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Apr-2023	6.1		https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf	A-SCH-STRU-030523/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists on a DCE endpoint through the logging capabilities of the webserver. Affected products: StruxureWare Data Center Expert (V7.9.2 and prior) **CVE ID : CVE-2023-25553**		
Vendor: shoppingfeed					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: shoppingfeed					
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.8.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	Shoppingfeed PrestaShop is an add-on to the PrestaShop ecommerce platform to synchronize data. The module Shoppingfeed for PrestaShop is vulnerable to SQL injection between version 1.4.0 and 1.8.2 due to a lack of input sanitization. This issue has been addressed in version 1.8.3. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28839**	https://github.com/shoppingflux/module-prestashop/security/advisories/GHSA-vfmq-w777-qvcf, https://github.com/shoppingflux/module-prestashop/pull/209	A-SHO-SHOP-030523/410
Vendor: Shopware					
Product: shopware					
Affected Version(s): 6.5.0.0					
Improper Control of Generation of Code ('Code Injection')	17-Apr-2023	8.8	Server-side Template Injection (SSTI) in Shopware 6 (<= v6.4.20.0, v6.5.0.0-rc1 <= v6.5.0.0-rc4), affecting both shopware/core and shopware/platform GitHub repositories, allows remote attackers with access to a Twig environment without the Sandbox extension to bypass the validation checks in	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-04-2023, https://github.com/shopware/platform/security/advisories/G	A-SHO-SHOP-030523/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`Shopware\Core\Framework\Adapter\Twig\SecurityExtension` and call any arbitrary PHP function and thus execute arbitrary code/commands via usage of fully-qualified names, supplied as array of strings, when referencing callables. Users are advised to upgrade to v6.4.20.1 to resolve this issue. This is a bypass of CVE-2023-22731. **CVE ID : CVE-2023-2017**	HSA-7v2v-9rm4-7m8f	
Affected Version(s): From (including) 6.1.0 Up to (including) 6.4.20.0					
Improper Control of Generation of Code ('Code Injection')	17-Apr-2023	8.8	Server-side Template Injection (SSTI) in Shopware 6 (<= v6.4.20.0, v6.5.0.0-rc1 <= v6.5.0.0-rc4), affecting both shopware/core and shopware/platform GitHub repositories, allows remote attackers with access to a Twig environment without the Sandbox extension to bypass the validation checks in `Shopware\Core\Framework\Adapter\Twig\SecurityExtension` and call any arbitrary PHP function and thus execute arbitrary code/commands via	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-04-2023, https://github.com/shopware/platform/security/advisories/GHSA-7v2v-9rm4-7m8f	A-SHO-SHOP-030523/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usage of fully-qualified names, supplied as array of strings, when referencing callables. Users are advised to upgrade to v6.4.20.1 to resolve this issue. This is a bypass of CVE-2023-22731. **CVE ID : CVE-2023-2017**		
Vendor: simple_pdf_viewer_project					
Product: simple_pdf_viewer					
Affected Version(s): * Up to (including) 1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	5.4	Auth. (contrinbutor+) Cross-Site Scripting (XSS) vulnerability in WebArea | Vera Nedvyzhenko Simple PDF Viewer plugin <= 1.9 versions. **CVE ID : CVE-2023-23817**	N/A	A-SIM-SIMP-030523/413
Vendor: simple_yearly_archive_project					
Product: simple_yearly_archive					
Affected Version(s): * Up to (excluding) 2.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Oliver Schlöbe Simple Yearly Archive plugin <= 2.1.8 versions. **CVE ID : CVE-2023-25484**	N/A	A-SIM-SIMP-030523/414
Vendor: sitemap_index_project					
Product: sitemap_index					
Affected Version(s): * Up to (including) 1.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Twardes Sitemap Index plugin <= 1.2.3 versions. **CVE ID : CVE-2023-23816**	N/A	A-SIT-SITE-030523/415
Vendor: smartlogix					
Product: wp-insert					
Affected Version(s): * Up to (excluding) 2.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in namithjawahar Wp-Insert plugin <= 2.5.0 versions. **CVE ID : CVE-2023-25461**	N/A	A-SMA-WP-I-030523/416
Vendor: snyk					
Product: advisor					
Affected Version(s): * Up to (excluding) 2023-03-28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2023	5.4	The Snyk Advisor website (https://snyk.io/advisor/) was vulnerable to a stored XSS prior to 28th March 2023. A feature of Snyk Advisor is to display the contents of a scanned package's Readme on its package health page. An attacker could create a package in NPM with an associated markdown README file	https://support.snyk.io/hc/en-us/articles/10146704933405	A-SNY-ADVI-030523/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			containing XSS-able HTML tags. Upon Snyk Advisor importing the package, the XSS would run each time an end user browsed to the package's page on Snyk Advisor. **CVE ID : CVE-2023-1767**		
Vendor: sqlparse_project					
Product: sqlparse					
Affected Version(s): From (including) 0.1.15 Up to (including) 0.4.4					
N/A	18-Apr-2023	7.5	sqlparse is a non-validating SQL parser module for Python. In affected versions the SQL parser contains a regular expression that is vulnerable to ReDoS (Regular Expression Denial of Service). This issue was introduced by commit `e75e358`. The vulnerability may lead to Denial of Service (DoS). This issues has been fixed in sqlparse 0.4.4 by commit `c457abd5f`. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-30608**	https://github.com/andialbrecht/sqlparse/security/advisories/GHSA-rrm6-wvj7-cwh2, https://github.com/andialbrecht/sqlparse/commit/c457abd5f097dd13fb21543381e7cfafe7d31cfb	A-SQL-SQLP-030523/418
Vendor: student_study_center_desk_management_system_project					
Product: student_study_center_desk_management_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file manage_student.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-226272. **CVE ID : CVE-2023-2151**	N/A	A-STU-STUD-030523/419
Externally Controlled Reference to a Resource in Another Sphere	18-Apr-2023	9.8	A vulnerability has been found in SourceCodester Student Study Center Desk Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument page leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-STU-STUD-030523/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier VDB-226273 was assigned to this vulnerability. **CVE ID : CVE-2023-2152**		
Vendor: task_reminder_system_project					
Product: task_reminder_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	7.2	A vulnerability, which was classified as critical, has been found in SourceCodester Task Reminder System 1.0. This issue affects some unknown processing of the file Master.php. 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-226271. **CVE ID : CVE-2023-2150**	N/A	A-TAS-TASK-030523/421
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Apr-2023	7.2	A vulnerability was found in SourceCodester Task Reminder System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/?page=reminders/view_reminder. The manipulation of	N/A	A-TAS-TASK-030523/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-226275. **CVE ID : CVE-2023-2154**		
Vendor: taxopress					
Product: taxopress					
Affected Version(s): * Up to (including) 3.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-2023	4.8	The TaxoPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Suggest Terms Title field in versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Editor+ permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2168**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2868795%40simple-tags%2Ftrunk&old=2774153%40simple-tags%2Ftrunk&sfp_email=&sfph_mail=	A-TAX-TAXO-030523/423
Improper Neutralization of Input During	19-Apr-2023	4.8	The TaxoPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Related Posts	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph	A-TAX-TAXO-030523/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			functionality in versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Editor+ permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2169**	_mail=&repo name=&new =2868795% 40simple-tags%2Ftrun k&old=2774 153%40sim ple-tags%2Ftrun k&sfp_email =&sfph_mail =	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-2023	4.8	The TaxoPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Related Posts functionality in versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with Editor+ permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2170**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&repo name=&new =2868795% 40simple-tags%2Ftrun k&old=2774 153%40sim ple-tags%2Ftrun k&sfp_email =&sfph_mail =	A-TAX-TAXO-030523/425
Vendor: theme_blvd_responsive_google_maps_project					
Product: theme_blvd_responsive_google_maps					
Affected Version(s): * Up to (including) 1.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Jason Bobich Theme Blvd Responsive Google Maps plugin <= 1.0.2 versions. **CVE ID : CVE-2023-22698**	N/A	A-THE-THEM-030523/426
Vendor: tinymce_custom_styles_project					
Product: tinymce_custom_styles					
Affected Version(s): * Up to (excluding) 1.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Tim Reeves & David Stöckl TinyMCE Custom Styles plugin <= 1.1.2 versions. **CVE ID : CVE-2023-23995**	N/A	A-TIN-TINY-030523/427
Vendor: transbank					
Product: transbank_webpay_rest					
Affected Version(s): * Up to (including) 1.6.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Apr-2023	7.2	Auth. (admin+) SQL Injection (SQLi) vulnerability in TransbankDevelopers Transbank Webpay REST plugin <= 1.6.6 versions. **CVE ID : CVE-2023-27610**	N/A	A-TRA-TRAN-030523/428
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 2.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	18-Apr-2023	4.3	Insufficient permission checks in the REST API in Tribe29 Checkmk <= 2.1.0p27 and <= 2.2.0b4 (beta) allow unauthorized users to schedule downtimes for any host. **CVE ID : CVE-2023-2020**	https://checkmk.com/werk/13981	A-TRI-CHEC-030523/429
Affected Version(s): 2.2.0					
Incorrect Authorization	18-Apr-2023	4.3	Insufficient permission checks in the REST API in Tribe29 Checkmk <= 2.1.0p27 and <= 2.2.0b4 (beta) allow unauthorized users to schedule downtimes for any host. **CVE ID : CVE-2023-2020**	https://checkmk.com/werk/13981	A-TRI-CHEC-030523/430
Affected Version(s): * Up to (excluding) 1.6.4					
Incorrect Permission Assignment for Critical Resource	18-Apr-2023	8.8	Privilege escalation in Tribe29 Checkmk Appliance before 1.6.4 allows authenticated site users to escalate privileges via incorrectly set permissions. **CVE ID : CVE-2023-22294**	https://checkmk.com/werk/9520	A-TRI-CHEC-030523/431
Vendor: ultimate_noindex_nofollow_tool_ii_project					
Product: ultimate_noindex_nofollow_tool_ii					
Affected Version(s): * Up to (including) 1.3					
Cross-Site Request	16-Apr-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kilian	N/A	A-ULT-ULTI-030523/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Evang Ultimate Noindex Nofollow Tool II plugin <= 1.3 versions. **CVE ID : CVE-2023-30474**		
Vendor: ultimate_wp_query_search_filter_project					
Product: ultimate_wp_query_search_filter					
Affected Version(s): * Up to (including) 1.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in TC Ultimate WP Query Search Filter plugin <= 1.0.10 versions. **CVE ID : CVE-2023-23832**	N/A	A-ULT-ULTI-030523/433
Vendor: uniguest					
Product: tripleplay					
Affected Version(s): 3.4.0					
Insufficiently Protected Credentials	19-Apr-2023	8.8	Incorrect Access Control in Tripleplay Platform releases prior to Caveman 3.4.0 allows authenticated user to modify other users passwords via a crafted request payload **CVE ID : CVE-2023-25760**	https://tripleplay.tv/wp-content/uploads/2023/03/CVE-2023-25760-Summary.pdf	A-UNI-TRIP-030523/434
Improper Neutralization of Input During Web Page Generation	19-Apr-2023	6.1	XSS vulnerability in TripleSign in Tripleplay Platform releases prior to Caveman 3.4.0 allows attackers to inject client-side code to run	https://tripleplay.tv/wp-content/uploads/2023/03/CVE-2023-26599-Summary.pdf	A-UNI-TRIP-030523/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			as an authenticated user via a crafted link. **CVE ID : CVE-2023-26599**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Apr-2023	5.4	OS Command Injection in TripleData Reporting Engine in Tripleplay Platform releases prior to Caveman 3.4.0 allows authenticated users to run unprivileged OS level commands via a crafted request payload. **CVE ID : CVE-2023-25759**	https://tripleplay.tv/wp-content/uploads/2023/03/CVE-2023-25759-Summary.pdf	A-UNI-TRIP-030523/436
Vendor: user_meta_manager_project					
Product: user_meta_manager					
Affected Version(s): * Up to (excluding) 3.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	6.1	Reflected Cross-Site Scripting (XSS) vulnerability in Jason Lau User Meta Manager plugin <= 3.4.9 versions. **CVE ID : CVE-2023-22718**	N/A	A-USE-USER-030523/437
Vendor: vegayazilim					
Product: mobile_assistant					
Affected Version(s): * Up to (excluding) 21.s.2343					
Improper Neutralization of Special Elements used in an SQL Command	17-Apr-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Veragroup Mobile Assistant allows SQL	N/A	A-VEG-MOBI-030523/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Injection.This issue affects Mobile Assistant: before 21.S.2343. **CVE ID : CVE-2023-1723**		
Vendor: vm2_project					
Product: vm2					
Affected Version(s): * Up to (including) 3.9.16					
N/A	17-Apr-2023	10	vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. There exists a vulnerability in exception sanitization of vm2 for versions up to 3.9.16, allowing attackers to raise an unsanitized host exception inside `handleException()` which can be used to escape the sandbox and run arbitrary code in host context. This vulnerability was patched in the release of version `3.9.17` of `vm2`. There are no known workarounds for this vulnerability. Users are advised to upgrade. **CVE ID : CVE-2023-30547**	https://github.com/patriksimek/vm2/commit/f3db4dee4d76b19869df05ba7880d638a880edd5, https://github.com/patriksimek/vm2/commit/4b22e87b102d97d45d112a0931dba1aef7eea049, https://github.com/patriksimek/vm2/security/advisories/GHSA-ch3r-j5x3-6q2m	A-VM2-VM2-030523/439
Vendor: w4_post_list_project					
Product: w4_post_list					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.4.6					
Missing Authorization	17-Apr-2023	6.5	The W4 Post List WordPress plugin before 2.4.6 does not ensure that password protected posts can be accessed before displaying their content, which could allow any authenticated users to access them **CVE ID : CVE-2023-1371**	N/A	A-W4_-W4_P-030523/440
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	6.1	The W4 Post List WordPress plugin before 2.4.6 does not escape some URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2023-1373**	N/A	A-W4_-W4_P-030523/441
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	5.4	The W4 Post List WordPress plugin before 2.4.6 does not validate and escape some of its block options before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0374**	N/A	A-W4_-W4_P-030523/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Wbce					
Product: wbce_cms					
Affected Version(s): 1.5.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Apr-2023	7.2	WBCE CMS 1.5.3 has a command execution vulnerability via admin/languages/install.php. **CVE ID : CVE-2023-29855**	N/A	A-WBC-WBCE-030523/443
Vendor: wc_fields_factory_project					
Product: wc_fields_factory					
Affected Version(s): * Up to (including) 4.1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Apr-2023	7.2	The WC Fields Factory WordPress plugin through 4.1.5 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin **CVE ID : CVE-2023-0277**	N/A	A-WC_-WC_F-030523/444
Vendor: winwar					
Product: inline_tweet_sharer					
Affected Version(s): * Up to (excluding) 2.6					
Improper Neutralization of Input During Web Page Generation	25-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Winwar Media Inline Tweet Sharer – Twitter Sharing Plugin	N/A	A-WIN-INLI-030523/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 2.5.3 versions. **CVE ID : CVE-2023-24005**		
Vendor: wordpress_custom_settings_project					
Product: wordpress_custom_settings					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Davinder Singh Custom Settings plugin <= 1.0 versions. **CVE ID : CVE-2023-23806**	N/A	A-WOR-WORD-030523/446
Vendor: wpchill					
Product: cpo_content_types					
Affected Version(s): * Up to (including) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPChill CPO Content Types plugin <= 1.1.0 versions. **CVE ID : CVE-2023-25451**	N/A	A-WPC-CPO_-030523/447
Vendor: Xwiki					
Product: Xwiki					
Affected Version(s): 14.6					
Improper Neutralization of Input During Web Page Generation	16-Apr-2023	6.1	XWiki Commons are technical libraries common to several other top level XWiki projects. It was possible to inject some code using the URL of authenticated	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-jjm5-5v9v-7hx2,	A-XWI-XWIK-030523/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			endpoints. This problem has been patched on XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29506**	https://github.com/xwiki/xwiki-platform/commit/1943ea26c967ef868fb5f67c487d98d97cba0380	
Affected Version(s): * Up to (excluding) 13.10.11					
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights `WikiManager.DeleteWiki` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `wikiId` url parameter. The problem has been patched on XWiki 13.10.11, 14.4.7, and 14.10. **CVE ID : CVE-2023-29211**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-w7v9-fc49-4qg4, https://github.com/xwiki/xwiki-platform/commit/ba4c76265b0b8a5e2218be400d18f08393fe1428#diff-64f39f5f2cc8c6560a44e21a5cfd509ef00e8a2157cd9847c9940a2e08ea43d1R63-R64	A-XWI-XWIK-030523/449
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki	https://github.com/xwiki/xwiki-platform/commit/50b4d91418b4150933f0317eb4a94ceaf5b69f67,	A-XWI-XWIK-030523/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to full access to the XWiki installation. The root cause is improper escaping of the included pages in the IncludedDocuments panel. The problem has been patched on XWiki 14.4.7, and 14.10. **CVE ID : CVE-2023-29214**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qx9h-c5v6-ghqh	
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `documentTree` macro parameters in This macro is installed by default in `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29509**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-f4v8-58f6-mwj4, https://github.com/xwiki/xwiki-platform/commit/80d5be36f700adcd56b6c8eb3ed8b973f62ec0ae, https://jira.xwiki.org/browse/XWIKI-20279	A-XWI-XWIK-030523/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the information loaded from attachments in `imported.vm`, `importinline.vm`, and `packagelist.vm`. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29512**	https://github.com/xwiki/xwiki-platform/commit/e4bbdc23fea0be4ef1921d1a58648028ce753344, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-hg5x-3w3x-7g96, https://jira.xwiki.org/browse/XWIKI-20267	A-XWI-XWIK-030523/452
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on any document (e.g., their own user profile) can execute code with	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9j36-3cp4-rh4j, https://jira.xwiki.org/bro	A-XWI-XWIK-030523/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			programming rights, leading to remote code execution. This vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29514**	wse/XWIKI-20268, https://github.com/xwiki/xwiki-platform/commit/7bf7094f8ffac095f5d66809af7554c9cc44de09	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights on `XWiki.AttachmentSelector` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping in the "Cancel and return to page" button. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. There are no known workarounds for this vulnerability.	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3989-4c6x-725f, https://github.com/xwiki/xwiki-platform/commit/aca1d677c58563bbe6e35c9e1c29fd8b12ebb996, https://jira.xwiki.org/browse/XWIKI-20275	A-XWI-XWIK-030523/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29516		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Invitation.InvitationCommon`. This page is installed by default. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-29518**	https://jira.xwiki.org/browse/XWIKI-20283, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-px54-3w5j-qjg9, https://github.com/xwiki/xwiki-platform/commit/3d055a0a5ec42fdebce4d71ee98f94553fdbfebf	A-XWI-XWIK-030523/455
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A registered user can perform remote code execution leading to privilege escalation by injecting the proper code in the "property" field of an attachment selector,	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3hjg-cghv-22ww, https://github.com/xwiki/xwiki-platform/commit/5e872	A-XWI-XWIK-030523/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as a gadget of their own dashboard. Note that the vulnerability does not impact comments of a wiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.2, 15.0-rc-1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29519**	5b4272cd3e5be09d3ca84273be2da6869c1, https://jira.xwiki.org/browse/XWIKI-20364	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Macro.VFSTreeMacro`. This page is not installed by default.This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.2, 14.4.8, 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	https://jira.xwiki.org/browse/XWIKI-20260, https://github.com/xwiki/xwiki-platform/commit/fad02328f5ec7ab7fe5b932ffb5bc5c1ba7a5b12, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-p67q-h88v-5jgr	A-XWI-XWIK-030523/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29521		
Exposure of Sensitive Information to an Unauthorized Actor	19-Apr-2023	7.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The office document viewer macro was allowing anyone to see any file content from the hosting server, provided that the office server was connected and depending on the permissions of the user running the servlet engine (e.g. tomcat) running XWiki. The same vulnerability also allowed to perform internal requests to resources from the hosting server. The problem has been patched in XWiki 13.10.11, 14.10.1, 14.4.8, 15.0-rc-1. Users are advised to upgrade. It might be possible to workaround this vulnerability by running XWiki in a sandbox with a user with very low privileges on the machine.	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-m3c3-9qj7-7xmx, https://jira.xwiki.org/browse/XWIKI-20449, https://jira.xwiki.org/browse/XWIKI-20447, https://jira.xwiki.org/browse/XWIKI-20324	A-XWI-XWIK-030523/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29517		
Improper Handling of Exceptional Conditions	19-Apr-2023	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to break many translations coming from wiki pages by creating a corrupted document containing a translation object. This will lead to a broken page. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no workarounds other than fixing any way to create a document that fail to load. **CVE ID : CVE-2023-29520**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9jq5-xwqw-q8j3, https://jira.xwiki.org/browse/XWIKI-20460	A-XWI-XWIK-030523/459
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2023	5.4	XWiki Commons are technical libraries common to several other top level XWiki projects. A user without script rights can introduce a stored XSS by using the Live Data macro, if the last author of the content of the page has script rights. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11.	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-hmm7-6ph9-8jf2, https://jira.xwiki.org/browse/XWIKI-20312	A-XWI-XWIK-030523/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29508		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user who can create a space can become admin of that space through App Within Minutes. The admin right implies the script right and thus allows JavaScript injection. The vulnerability can be exploited by creating an app in App Within Minutes. If the button should be disabled because the user doesn't have global edit right, the app can also be created by directly opening `/xwiki/bin/view/AppWithinMinutes/CreateApplication?wizard=true` on the XWiki installation. This has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1 by not granting the space admin right if the user doesn't have script right on the space where the app is created. Error message are displayed to warn the user that	https://github.com/xwiki/xwiki-platform/commit/e73b890623efa604adc484ad82f37e31596fe1a6, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-44h9-xxvx-pg6x, https://jira.xwiki.org/browse/XWIKI-20190	A-XWI-XWIK-030523/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the app will be broken in this case. Users who became space admin through this vulnerability won't loose the space admin right due to the fix, so it is advised to check if all users who created AWM apps should keep their space admin rights. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29515**		
Affected Version(s): * Up to (excluding) 14.10.1					
Improper Access Control	19-Apr-2023	4.3	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. If guest has view right on any document. It's possible to create a new user using the `distribution/firstadminuser.wiki` in the wrong context. This vulnerability has been patched in XWiki 15.0-rc-1 and 14.10.1. There is no known workaround other than upgrading. **CVE ID : CVE-2023-29513**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-fp36-mjw5-fmgx, https://jira.xwiki.org/browse/XWIKI-19852, https://jira.xwiki.org/browse/XWIKI-20400	A-XWI-XWIK-030523/462
Affected Version(s): * Up to (excluding) 14.10.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In XWiki, every user can add translations that are only applied to the current user. This also allows overriding existing translations. Such translations are often included in privileged contexts without any escaping which allows remote code execution for any user who has edit access on at least one document which could be the user's own profile where edit access is enabled by default. A mitigation for this vulnerability is part of XWiki 14.10.2 and XWiki 15.0 RC1: translations with user scope now require script right. This means that regular users cannot exploit this anymore as users don't have script right by default anymore starting with XWiki 14.10. There are no known workarounds apart from upgrading to a patched versions. **CVE ID : CVE-2023-29510**	https://github.com/xwiki/xwiki-platform/commit/d06ff8a58480abc7f63eb1d4b8b366024d990643, https://jira.xwiki.org/browse/XWIKI-19749, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-4v38-964c-xjmw	A-XWI-XWIK-030523/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14.4.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. The attack works by opening a non-existing page with a name crafted to contain a dangerous payload. This issue has been patched in XWiki 14.4.8, 14.10.3 and 15.0RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29522**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-mjw9-3f9f-jq2w, https://jira.xwiki.org/browse/XWIKI-20456, https://github.com/xwiki/xwiki-platform/commit/d7e56185376641ee5d66477c6b2791ca8e85cfee	A-XWI-XWIK-030523/464
Affected Version(s): 14.0					
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity	https://jira.xwiki.org/browse/XWIKI-20261, https://github.com/xwiki/xwiki-platform/commit/f1e310826a19acdcdecdecdcfe	A-XWI-XWIK-030523/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the section ids in `XWiki.AdminFieldsDisplaySheet`. This page is installed by default. The vulnerability has been patched in XWiki versions 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. **CVE ID : CVE-2023-29511**	171d21f24d6ede, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rfh6-mg6h-h668	
Affected Version(s): 14.10					
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights `WikiManager.DeleteWiki` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `wikiId` url parameter. The problem has been patched on XWiki 13.10.11, 14.4.7, and 14.10. **CVE ID : CVE-2023-29211**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-w7v9-fc49-4qg4, https://github.com/xwiki/xwiki-platform/commit/ba4c76265b0b8a5e2218be400d18f08393fe1428#diff-64f39f5f2cc8c6560a44e21a5cfd509ef00e8a2157cd9847c9940a2e08ea43d1R63-R64	A-XWI-XWIK-030523/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the included pages in the included documents edit panel. The problem has been patched on XWiki 14.4.7, and 14.10. **CVE ID : CVE-2023-29212**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-c5f4-p5wv-2475, https://github.com/xwiki/xwiki-platform/commit/22f249a0eb9f2a64214628217e812a994419b69f#diff-a51a252f019027446402734 2b4e3eafc4ae32de4d9c17ef166e54fc5454c5689R214-R217	A-XWI-XWIK-030523/467
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the included pages in the IncludedDocuments panel. The problem has been patched on	https://github.com/xwiki/xwiki-platform/commit/50b4d91418b4150933f0317eb4a94ceaf5b69f67, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-qx9h-c5v6-ghqh	A-XWI-XWIK-030523/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XWiki 14.4.7, and 14.10. **CVE ID : CVE-2023-29214**		
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `documentTree` macro parameters in This macro is installed by default in `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29509**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-f4v8-58f6-mwj4, https://github.com/xwiki/xwiki-platform/commit/80d5be36f700adcd56b6c8eb3ed8b973f62ec0ae, https://jira.xwiki.org/browse/XWIKI-20279	A-XWI-XWIK-030523/469
N/A	16-Apr-2023	7.2	XWiki Commons are technical libraries common to several other top level XWiki projects. The Document script API returns directly a DocumentAuthors allowing to set any	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-pwfv-3cvg-9m4c, https://githu	A-XWI-XWIK-030523/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authors to the document, which in consequence can allow subsequent executions of scripts since this author is used for checking rights. The problem has been patched in XWiki 14.10 and 14.4.7 by returning a safe script API. **CVE ID : CVE-2023-29507**	b.com/xwiki/xwiki-platform/commit/905cdd7c421dbf8c565557cdc773ab1aa9028f83	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2023	6.1	XWiki Commons are technical libraries common to several other top level XWiki projects. It was possible to inject some code using the URL of authenticated endpoints. This problem has been patched on XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29506**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-jjm5-5v9v-7hx2, https://github.com/xwiki/xwiki-platform/commit/1943ea26c967ef868fb5f67c487d98d97cba0380	A-XWI-XWIK-030523/471
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Apr-2023	5.4	XWiki Commons are technical libraries common to several other top level XWiki projects. A user without script rights can introduce a stored XSS by using the Live Data macro, if the last author of the content of the page has script rights. This has been	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-hmm7-6ph9-8jf2, https://jira.xwiki.org/browse/XWIKI-20312	A-XWI-XWIK-030523/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in XWiki 14.10, 14.4.7, and 13.10.11. **CVE ID : CVE-2023-29508**		
Affected Version(s): From (excluding) 14.0 Up to (excluding) 14.4.8					
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the section ids in `XWiki.AdminFieldsDisplaySheet`. This page is installed by default. The vulnerability has been patched in XWiki versions 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. **CVE ID : CVE-2023-29511**	https://jira.xwiki.org/browse/XWIKI-20261, https://github.com/xwiki/xwiki-platform/commit/f1e310826a19acdcdecdecdcfe171d21f24d6ede, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rfh6-mg6h-h668	A-XWI-XWIK-030523/473
Affected Version(s): From (including) 1.7 Up to (excluding) 13.10.11					
Improper Neutralization of Directives in Dynamically	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page	https://jira.xwiki.org/browse/XWIKI-20261, https://github.com/xwiki/xwiki-	A-XWI-XWIK-030523/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Evaluated Code ('Eval Injection')			(e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the section ids in `XWiki.AdminFieldsDisplaySheet`. This page is installed by default. The vulnerability has been patched in XWiki versions 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. **CVE ID : CVE-2023-29511**	platform/commit/f1e310826a19acdcdecdecdcfe171d21f24d6ede, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rfh6-mg6h-h668	
Affected Version(s): From (including) 10.11.1 Up to (excluding) 13.10.11					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to display or interact with any page a user cannot access through the combination of the async and display macros. A comment with either macro will be executed when viewed providing a code injection vector in the context of the running server. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.3, 14.4.8,	https://jira.xwiki.org/browse/XWIKI-20394, https://jira.xwiki.org/browse/XRENDERING-694, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gpq5-7p34-vqx5	A-XWI-XWIK-030523/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and 13.10.11. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-29526**		
Affected Version(s): From (including) 12.6.6 Up to (excluding) 13.10.11					
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with the right to add an object on a page can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the styles properties `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki versions 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-30537**	https://github.com/xwiki/xwiki-platform/commit/df596f15368342236f8899ca122af8f3df0fe2e8, https://jira.xwiki.org/browse/XWIKI-20280, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vrr8-fp7c-7qgp	A-XWI-XWIK-030523/476
Affected Version(s): From (including) 13.10.8 Up to (excluding) 13.10.11					
Improper Neutralization of Input During Web Page	16-Apr-2023	6.1	XWiki Commons are technical libraries common to several other top level XWiki projects. It was possible to inject some	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-	A-XWI-XWIK-030523/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			code using the URL of authenticated endpoints. This problem has been patched on XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29506**	jjm5-5v9v-7hx2, https://github.com/xwiki/xwiki-platform/commit/1943ea26c967ef868fb5f67c487d98d97cba0380	
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.7					
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the included pages in the included documents edit panel. The problem has been patched on XWiki 14.4.7, and 14.10. **CVE ID : CVE-2023-29212**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-c5f4-p5wv-2475, https://github.com/xwiki/xwiki-platform/commit/22f249a0eb9f2a64214628217e812a994419b69f#diff-a51a252f019027446402 7342b4e3eafc4ae32de4d9c17ef166e54fc5454c5689R214-R217	A-XWI-XWIK-030523/478
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with the right to add an	https://github.com/xwiki/xwiki-platform/commit/df596f15368342236f8899ca122	A-XWI-XWIK-030523/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			object on a page can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the styles properties `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki versions 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-30537**	af8f3df0fe2e8, https://jira.xwiki.org/browse/XWIKI-20280, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vrr8-fp7c-7qgp	
Affected Version(s): From (including) 14.0 Up to (excluding) 14.4.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the information loaded from attachments in `imported.vm`, `importinline.vm`, and `packagelist.vm`. This page is installed by	https://github.com/xwiki/xwiki-platform/commit/e4bbdc23fea0be4ef1921d1a58648028ce753344, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-hg5x-3w3x-7g96, https://jira.xwiki.org/browse/XWIKI-20267	A-XWI-XWIK-030523/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29512**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on any document (e.g., their own user profile) can execute code with programming rights, leading to remote code execution. This vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29514**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9j36-3cp4-rh4j, https://jira.xwiki.org/browse/XWIKI-20268, https://github.com/xwiki/xwiki-platform/commit/7bf7094f8ffac095f5d66809af7554c9cc44de09	A-XWI-XWIK-030523/481
Improper Neutralization of Special Elements in Output Used by a Downstream	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights on `XWiki.AttachmentSelector` can execute	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3989-4c6x-725f, https://githu	A-XWI-XWIK-030523/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping in the "Cancel and return to page" button. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29516**	b.com/xwiki/xwiki-platform/commit/aca1d677c58563bbe6e35c9e1c29fd8b12ebb996, https://jira.xwiki.org/browse/XWIKI-20275	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Invitation.InvitationCommon`. This page is installed by default. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11.	https://jira.xwiki.org/browse/XWIKI-20283, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-px54-3w5j-qjg9, https://github.com/xwiki/xwiki-platform/commit/3d055a0a5ec42fdebce4d71ee98f94553fdbfebf	A-XWI-XWIK-030523/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-29518**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A registered user can perform remote code execution leading to privilege escalation by injecting the proper code in the "property" field of an attachment selector, as a gadget of their own dashboard. Note that the vulnerability does not impact comments of a wiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.2, 15.0-rc-1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29519**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3hjg-cghv-22ww, https://github.com/xwiki/xwiki-platform/commit/5e8725b4272cd3e5be09d3ca84273be2da6869c1, https://jira.xwiki.org/browse/XWIKI-20364	A-XWI-XWIK-030523/484
Improper Neutralization of Special Elements in Output Used by a Downstream	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or	https://jira.xwiki.org/browse/XWIKI-20260, https://github.com/xwiki/xwiki-platform/commit/fad02	A-XWI-XWIK-030523/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Macro.VFSTreeMacro`. This page is not installed by default.This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.2, 14.4.8, 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29521**	328f5ec7ab7fe5b932ffb5bc5c1ba7a5b12, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-p67q-h88v-5jgr	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to display or interact with any page a user cannot access through the combination of the async and display macros. A comment with either macro will be executed when viewed providing a code injection vector in the context of the running server. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.3, 14.4.8, and 13.10.11. Users	https://jira.xwiki.org/browse/XWIKI-20394, https://jira.xwiki.org/browse/XRENDERING-694, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gpq5-7p34-vqx5	A-XWI-XWIK-030523/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-29526**		
Exposure of Sensitive Information to an Unauthorized Actor	19-Apr-2023	7.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The office document viewer macro was allowing anyone to see any file content from the hosting server, provided that the office server was connected and depending on the permissions of the user running the servlet engine (e.g. tomcat) running XWiki. The same vulnerability also allowed to perform internal requests to resources from the hosting server. The problem has been patched in XWiki 13.10.11, 14.10.1, 14.4.8, 15.0-rc-1. Users are advised to upgrade. It might be possible to workaround this vulnerability by running XWiki in a sandbox with a user with very low	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-m3c3-9qj7-7xmx, https://jira.xwiki.org/browse/XWIKI-20449, https://jira.xwiki.org/browse/XWIKI-20447, https://jira.xwiki.org/browse/XWIKI-20324	A-XWI-XWIK-030523/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on the machine. **CVE ID : CVE-2023-29517**		
Improper Handling of Exceptional Conditions	19-Apr-2023	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to break many translations coming from wiki pages by creating a corrupted document containing a translation object. This will lead to a broken page. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no workarounds other than fixing any way to create a document that fail to load. **CVE ID : CVE-2023-29520**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9jq5-xwqw-q8j3, https://jira.xwiki.org/browse/XWIKI-20460	A-XWI-XWIK-030523/488
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Apr-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user who can create a space can become admin of that space through App Within Minutes. The	https://github.com/xwiki/xwiki-platform/commit/e73b890623efa604adc484ad82f37e31596fe1a6, https://githu	A-XWI-XWIK-030523/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admin right implies the script right and thus allows JavaScript injection. The vulnerability can be exploited by creating an app in App Within Minutes. If the button should be disabled because the user doesn't have global edit right, the app can also be created by directly opening `/xwiki/bin/view/AppWithinMinutes/CreateApplication?wizard=true` on the XWiki installation. This has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1 by not granting the space admin right if the user doesn't have script right on the space where the app is created. Error message are displayed to warn the user that the app will be broken in this case. Users who became space admin through this vulnerability won't loose the space admin right due to the fix, so it is advised to check if all users who created AWM apps should keep their space admin rights. Users are advised to upgrade. There are no	b.com/xwiki/xwiki-platform/security/advisories/GHSA-44h9-xxvx-pg6x, https://jira.xwiki.org/browse/XWIKI-20190	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known workarounds for this vulnerability. **CVE ID : CVE-2023-29515**		
Affected Version(s): From (including) 14.4.0 Up to (excluding) 14.4.7					
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights `WikiManager.DeleteWiki` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `wikiId` url parameter. The problem has been patched on XWiki 13.10.11, 14.4.7, and 14.10. **CVE ID : CVE-2023-29211**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-w7v9-fc49-4qg4, https://github.com/xwiki/xwiki-platform/commit/ba4c76265b0b8a5e2218be400d18f08393fe1428#diff-64f39f5f2cc8c6560a44e21a5cfd509ef00e8a2157cd9847c9940a2e08ea43d1R63-R64	A-XWI-XWIK-030523/490
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with edit rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the	https://github.com/xwiki/xwiki-platform/commit/50b4d91418b4150933f0317eb4a94ceaf5b69f67, https://github.com/xwiki/xwiki-platform/security/adviso	A-XWI-XWIK-030523/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			included pages in the IncludedDocuments panel. The problem has been patched on XWiki 14.4.7, and 14.10. **CVE ID : CVE-2023-29214**	ries/GHSA-qx9h-c5v6-ghqh	
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Commons are technical libraries common to several other top level XWiki projects. Any user with view rights on commonly accessible documents can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the `documentTree` macro parameters in This macro is installed by default in `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29509**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-f4v8-58f6-mwj4, https://github.com/xwiki/xwiki-platform/commit/80d5be36f700adcd56b6c8eb3ed8b973f62ec0ae, https://jira.xwiki.org/browse/XWIKI-20279	A-XWI-XWIK-030523/492
Improper Neutralization of Input During	16-Apr-2023	5.4	XWiki Commons are technical libraries common to several other top level XWiki projects. A user	https://github.com/xwiki/xwiki-platform/security/adviso	A-XWI-XWIK-030523/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			without script rights can introduce a stored XSS by using the Live Data macro, if the last author of the content of the page has script rights. This has been patched in XWiki 14.10, 14.4.7, and 13.10.11. **CVE ID : CVE-2023-29508**	ries/GHSA-hmm7-6ph9-8jf2, https://jira.xwiki.org/browse/XWIKI-20312	
Affected Version(s): From (including) 14.4.1 Up to (excluding) 14.4.7					
N/A	16-Apr-2023	7.2	XWiki Commons are technical libraries common to several other top level XWiki projects. The Document script API returns directly a DocumentAuthors allowing to set any authors to the document, which in consequence can allow subsequent executions of scripts since this author is used for checking rights. The problem has been patched in XWiki 14.10 and 14.4.7 by returning a safe script API. **CVE ID : CVE-2023-29507**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-pwfv-3cvg-9m4c, https://github.com/xwiki/xwiki-platform/commit/905cdd7c421dbf8c565557cdc773ab1aa9028f83	A-XWI-XWIK-030523/494
Affected Version(s): From (including) 14.4.3 Up to (excluding) 14.4.7					
Improper Neutralization of Input	16-Apr-2023	6.1	XWiki Commons are technical libraries common to several other top level XWiki	https://github.com/xwiki/xwiki-platform/sec	A-XWI-XWIK-030523/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			projects. It was possible to inject some code using the URL of authenticated endpoints. This problem has been patched on XWiki 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-29506**	urity/advisories/GHSA-jjm5-5v9v-7hx2, https://github.com/xwiki/xwiki-platform/commit/1943ea26c967ef868fb5f67c487d98d97cba0380	
Affected Version(s): From (including) 14.5 Up to (excluding) 14.10					
Improper Control of Generation of Code ('Code Injection')	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with the right to add an object on a page can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the styles properties `FlamingoThemesCode.WebHome`. This page is installed by default. The vulnerability has been patched in XWiki versions 13.10.11, 14.4.7 and 14.10. **CVE ID : CVE-2023-30537**	https://github.com/xwiki/xwiki-platform/commit/df596f15368342236f8899ca122af8f3df0fe2e8, https://jira.xwiki.org/browse/XWIKI-20280, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-vrr8-fp7c-7qgp	A-XWI-XWIK-030523/496
Affected Version(s): From (including) 14.5 Up to (excluding) 14.10.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	16-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the section ids in `XWiki.AdminFieldsDisplaySheet`. This page is installed by default. The vulnerability has been patched in XWiki versions 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. **CVE ID : CVE-2023-29511**	https://jira.xwiki.org/browse/XWIKI-20261, https://github.com/xwiki/xwiki-platform/commit/f1e310826a19acdcdecdecdcfe171d21f24d6ede, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rfh6-mg6h-h668	A-XWI-XWIK-030523/497
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on a page (e.g., it's own user page), can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of the	https://github.com/xwiki/xwiki-platform/commit/e4bbdc23fea0be4ef1921d1a58648028ce753344, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-hg5x-3w3x-	A-XWI-XWIK-030523/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information loaded from attachments in `imported.vm`, `importinline.vm`, and `packagelist.vm`. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29512**	7g96, https://jira.xwiki.org/browse/XWIKI-20267	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with edit rights on any document (e.g., their own user profile) can execute code with programming rights, leading to remote code execution. This vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29514**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9j36-3cp4-rh4j, https://jira.xwiki.org/browse/XWIKI-20268, https://github.com/xwiki/xwiki-platform/commit/7bf7094f8ffac095f5d66809af7554c9cc44de09	A-XWI-XWIK-030523/499
Improper Neutralization of	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime	https://github.com/xwiki/xwiki-	A-XWI-XWIK-030523/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			services for applications built on top of it. Any user with view rights on `XWiki.AttachmentSelector` can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping in the "Cancel and return to page" button. This page is installed by default. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29516**	platform/security/advisories/GHSA-3989-4c6x-725f, https://github.com/xwiki/xwiki-platform/commit/aca1d677c58563bbe6e35c9e1c29fd8b12ebb996, https://jira.xwiki.org/browse/XWIKI-20275	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Invitation.InvitationC	https://jira.xwiki.org/browse/XWIKI-20283, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-px54-3w5j-qjg9, https://github.com/xwiki/xwiki-platform/co	A-XWI-XWIK-030523/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ommon`. This page is installed by default. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-29518**	mmit/3d055a0a5ec42fdebce4d71ee98f94553fdbfebf	
Exposure of Sensitive Information to an Unauthorized Actor	19-Apr-2023	7.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The office document viewer macro was allowing anyone to see any file content from the hosting server, provided that the office server was connected and depending on the permissions of the user running the servlet engine (e.g. tomcat) running XWiki. The same vulnerability also allowed to perform internal requests to resources from the hosting server. The problem has been patched in XWiki 13.10.11, 14.10.1, 14.4.8, 15.0-rc-1. Users are advised to upgrade. It might be	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-m3c3-9qj7-7xmx, https://jira.xwiki.org/browse/XWIKI-20449, https://jira.xwiki.org/browse/XWIKI-20447, https://jira.xwiki.org/browse/XWIKI-20324	A-XWI-XWIK-030523/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to workaround this vulnerability by running XWiki in a sandbox with a user with very low privileges on the machine. **CVE ID : CVE-2023-29517**		
Improper Handling of Exceptional Conditions	19-Apr-2023	6.5	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to break many translations coming from wiki pages by creating a corrupted document containing a translation object. This will lead to a broken page. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.1, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no workarounds other than fixing any way to create a document that fail to load. **CVE ID : CVE-2023-29520**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-9jq5-xwqw-q8j3, https://jira.xwiki.org/browse/XWIKI-20460	A-XWI-XWIK-030523/503
Improper Neutralization of Input	19-Apr-2023	5.4	XWiki Platform is a generic wiki platform offering runtime services for	https://github.com/xwiki/xwiki-platform/co	A-XWI-XWIK-030523/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			applications built on top of it. Any user who can create a space can become admin of that space through App Within Minutes. The admin right implies the script right and thus allows JavaScript injection. The vulnerability can be exploited by creating an app in App Within Minutes. If the button should be disabled because the user doesn't have global edit right, the app can also be created by directly opening `/xwiki/bin/view/AppWithinMinutes/CreateApplication?wizard=true` on the XWiki installation. This has been patched in XWiki 13.10.11, 14.4.8, 14.10.1 and 15.0 RC1 by not granting the space admin right if the user doesn't have script right on the space where the app is created. Error message are displayed to warn the user that the app will be broken in this case. Users who became space admin through this vulnerability won't loose the space admin right due to the fix, so it is advised to check if	mmit/e73b890623efa604adc484ad82f37e31596fe1a6, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-44h9-xxvx-pg6x, https://jira.xwiki.org/browse/XWIKI-20190	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all users who created AWM apps should keep their space admin rights. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29515**		
Affected Version(s): From (including) 14.5 Up to (excluding) 14.10.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A registered user can perform remote code execution leading to privilege escalation by injecting the proper code in the "property" field of an attachment selector, as a gadget of their own dashboard. Note that the vulnerability does not impact comments of a wiki. The vulnerability has been patched in XWiki 13.10.11, 14.4.8, 14.10.2, 15.0-rc-1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29519**	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-3hjg-cghv-22ww, https://github.com/xwiki/xwiki-platform/commit/5e8725b4272cd3e5be09d3ca84273be2da6869c1, https://jira.xwiki.org/browse/XWIKI-20364	A-XWI-XWIK-030523/505
Improper Neutralization of	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime	https://jira.xwiki.org/browse/XWIKI-	A-XWI-XWIK-030523/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			services for applications built on top of it. Any user with view rights can execute arbitrary Groovy, Python or Velocity code in XWiki leading to full access to the XWiki installation. The root cause is improper escaping of `Macro.VFSTreeMacro`. This page is not installed by default.This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.2, 14.4.8, 13.10.11. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29521**	20260, https://github.com/xwiki/xwiki-platform/commit/fad02328f5ec7ab7fe5b932ffb5bc5c1ba7a5b12, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-p67q-h88v-5jgr	
Affected Version(s): From (including) 14.5 Up to (excluding) 14.10.3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Any user with view rights can execute arbitrary script macros including Groovy and Python macros that allow remote code execution including unrestricted read and write access to all wiki contents. The attack	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-mjw9-3f9f-jq2w, https://jira.xwiki.org/browse/XWIKI-20456, https://github.com/xwiki/xwiki-platform/co	A-XWI-XWIK-030523/507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			works by opening a non-existing page with a name crafted to contain a dangerous payload. This issue has been patched in XWiki 14.4.8, 14.10.3 and 15.0RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-29522**	mmit/d7e56185376641ee5d66477c6b2791ca8e85cfee	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Apr-2023	8.8	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to display or interact with any page a user cannot access through the combination of the async and display macros. A comment with either macro will be executed when viewed providing a code injection vector in the context of the running server. This vulnerability has been patched in XWiki 15.0-rc-1, 14.10.3, 14.4.8, and 13.10.11. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-29526**	https://jira.xwiki.org/browse/XWIKI-20394, https://jira.xwiki.org/browse/XRENDERING-694, https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-gpq5-7p34-vqx5	A-XWI-XWIK-030523/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: yikesinc					
Product: easy_forms_for_mailchimp					
Affected Version(s): * Up to (excluding) 6.8.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Apr-2023	5.4	The Easy Forms for Mailchimp WordPress plugin before 6.8.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2023-1325**	N/A	A-YIK-EASY-030523/509
Hardware					
Vendor: Dlink					
Product: dir-823g					
Affected Version(s): -					
Out-of-bounds Write	17-Apr-2023	9.8	D-Link DIR823G_V1.0.2B05 was discovered to contain a stack overflow via the NewPassword parameters in SetPasswdSettings. **CVE ID : CVE-2023-29665**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--030523/510
Vendor: electra-air					
Product: central_ac_unit					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	17-Apr-2023	9.8	Electra Central AC unit – Hardcoded Credentials in unspecified code used by the unit. **CVE ID : CVE-2023-24501**	N/A	H-ELE-CENT-030523/511
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to load unauthorized FW. **CVE ID : CVE-2023-24500**	N/A	H-ELE-CENT-030523/512
Inadequate Encryption Strength	17-Apr-2023	6.5	Electra Central AC unit – The unit opens an AP with an easily calculated password. **CVE ID : CVE-2023-24502**	N/A	H-ELE-CENT-030523/513
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to connect to unauthorized update server. **CVE ID : CVE-2023-24504**	N/A	H-ELE-CENT-030523/514
Vendor: Juniper					
Product: acx1000					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX1-030523/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx1100					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the	https://supportportal.juniper.net/JSA70586	H-JUN-ACX1-030523/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28961		
Product: acx2000					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	H-JUN-ACX2-030523/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx2100					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX2-030523/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx2200					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the	https://supportportal.juniper.net/JSA70586	H-JUN-ACX2-030523/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28961		
Product: acx4000					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	H-JUN-ACX4-030523/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx500					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx5000					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28961		
Product: acx5048					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx5096					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx5400					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28961		
Product: acx5448					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx5800					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX5-030523/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx6300					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the	https://supportportal.juniper.net/JSA70586	H-JUN-ACX6-030523/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28961		
Product: acx6360					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	H-JUN-ACX6-030523/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx710					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX7-030523/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx7100-32c					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the	https://supportportal.juniper.net/JSA70586	H-JUN-ACX7-030523/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28961		
Product: acx7100-48l					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	H-JUN-ACX7-030523/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: acx7509					
Affected Version(s): -					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah'	https://supportportal.juniper.net/JSA70586	H-JUN-ACX7-030523/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Product: jrr200					
Affected Version(s): -					
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered	https://supportportal.juniper.net/JSA70594	H-JUN-JRR2-030523/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Product: mx					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed	https://supportportal.juniper.net/JSA70599	H-JUN-MX-030523/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx10					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled:	https://supportportal.juniper.net/JSA70599	H-JUN-MX10-030523/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx10000					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of	https://supportportal.juniper.net/JSA70599	H-JUN-MX10-030523/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx10003					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS	https://supportportal.juniper.net/JSA70599	H-JUN-MX10-030523/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx10008					
Affected Version(s): -					
Improper Check for Unusual or Exceptiona	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the	https://supportportal.juniper.net/JSA70599	H-JUN-MX10-030523/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx10016					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions	https://supportportal.juniper.net/JSA70599	H-JUN-MX10-030523/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx104					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions	https://supportportal.juniper.net/JSA70599	H-JUN-MX10-030523/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx150					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet	https://supportportal.juniper.net/JSA70599	H-JUN-MX15-030523/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx2008					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_L	https://supportportal.juniper.net/JSA70599	H-JUN-MX20-030523/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx2010					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a	https://supportportal.juniper.net/JSA70599	H-JUN-MX20-030523/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx2020					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this	https://supportportal.juniper.net/JSA70599	H-JUN-MX20-030523/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx204					
Affected Version(s): -					
Improper Check for Unusual or Exceptiona	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper	https://supportportal.juniper.net/JSA70599	H-JUN-MX20-030523/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx240					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting,	https://supportportal.juniper.net/JSA70599	H-JUN-MX24-030523/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx40					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11;	https://supportportal.juniper.net/JSA70599	H-JUN-MX40-030523/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx480					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the	https://supportportal.juniper.net/JSA70599	H-JUN-MX48-030523/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx5					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_L	https://supportportal.juniper.net/JSA70599	H-JUN-MX5-030523/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx80					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a	https://supportportal.juniper.net/JSA70599	H-JUN-MX80-030523/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: mx960					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this	https://supportportal.juniper.net/JSA70599	H-JUN-MX96-030523/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Product: nfx150					
Affected Version(s): -					
Improper Link Resolution Before File Access	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX	https://supportportal.juniper.net/JSA70596	H-JUN-NFX1-030523/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Link Following')			Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
Product: nfx250					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass	https://supportportal.juniper.net/JSA70596	H-JUN-NFX2-030523/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: nfx350					
Affected Version(s): -					
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2	https://supportportal.juniper.net/JSA70596	H-JUN-NFX3-030523/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
Product: ptx1000					
Affected Version(s): -					
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames	https://supportportal.juniper.net/JSA70612	H-JUN-PTX1-030523/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Product: qfx10000					
Affected Version(s): -					
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an	https://supportportal.juniper.net/JSA70612	H-JUN-QFX1-030523/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Product: qfx10002					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to	https://supportportal.juniper.net/JSA70589	H-JUN-QFX1-030523/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2	https://supportportal.juniper.net/JSA70612	H-JUN-QFX1-030523/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger	https://supportportal.juniper.net/JSA70584	H-JUN-QFX1-030523/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Product: qfx10008					
Affected Version(s): -					
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This	https://supportportal.juniper.net/JSA70612	H-JUN-QFX1-030523/561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Product: qfx10016					
Affected Version(s): -					
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS).	https://supportportal.juniper.net/JSA70612	H-JUN-QFX1-030523/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Product: srx100					
Affected Version(s): -					
Allocation of Resources Without	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks	https://supportportal.juniper.net/JSA70592	H-JUN-SRX1-030523/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx110					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security	https://supportportal.juniper.net/JSA70592	H-JUN-SRX1-030523/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx1400					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-	https://supportportal.juniper.net/JSA70592	H-JUN-SRX1-030523/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx1500					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder	https://supportportal.juniper.net/JSA70592	H-JUN-SRX1-030523/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx210					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix	https://supportportal.juniper.net/JSA70592	H-JUN-SRX2-030523/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx220					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic	https://supportportal.juniper.net/JSA70592	H-JUN-SRX2-030523/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx240					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature	https://supportportal.juniper.net/JSA70592	H-JUN-SRX2-030523/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx240h2					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX2-030523/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx240m					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX2-030523/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx300					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx320					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx340					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx3400					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx345					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx3600					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx380					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX3-030523/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx4000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX4-030523/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx4100					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX4-030523/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx4200					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX4-030523/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx4600					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX4-030523/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx5000					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx5400					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx550					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx550m					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx550_hm					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Product: srx5600					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID:	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx5800					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this	https://supportportal.juniper.net/JSA70592	H-JUN-SRX5-030523/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Product: srx650					
Affected Version(s): -					
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	H-JUN-SRX6-030523/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Vendor: Nvidia					
Product: dgx-1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2023	8.8	NVIDIA DGX-1 BMC contains a vulnerability in the SPX REST API, where an attacker with the appropriate level of authorization can inject arbitrary shell commands, which may lead to code execution, denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-25507**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	H-NVI-DGX--030523/591
Out-of-bounds Write	22-Apr-2023	8.2	NVIDIA DGX-1 contains a vulnerability in Ofbd in AMI SBIOS, where a preconditioned heap can allow a user with elevated privileges to cause an access beyond the end of a buffer, which may lead to code execution, escalation of privileges, denial of service and information disclosure. The scope of the impact of this vulnerability can extend to other components.	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	H-NVI-DGX--030523/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25506		
Improper Authentication	22-Apr-2023	7.8	NVIDIA DGX-1 SBIOS contains a vulnerability in the Uncore PEI module, where authentication of the code executed by SSA is missing, which may lead to arbitrary code execution, denial of service, escalation of privileges assisted by a firmware implant, information disclosure assisted by a firmware implant, data tampering, and SecureBoot bypass. **CVE ID : CVE-2023-0209**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	H-NVI-DGX--030523/593
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Apr-2023	7.8	NVIDIA DGX-1 BMC contains a vulnerability in the IPMI handler of the AMI MegaRAC BMC , where an attacker with the appropriate level of authorization can cause a buffer overflow, which may lead to denial of service, information disclosure, or arbitrary code execution. **CVE ID : CVE-2023-25505**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	H-NVI-DGX--030523/594
Improper Limitation of a	22-Apr-2023	7.8	NVIDIA DGX-1 BMC contains a vulnerability in the	https://nvidia.custhelp.com/app/answ	H-NVI-DGX--030523/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			IPMI handler, where an attacker with the appropriate level of authorization can upload and download arbitrary files under certain circumstances, which may lead to denial of service, escalation of privileges, information disclosure, and data tampering. **CVE ID : CVE-2023-25508**	ers/detail/a_id/5458	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Apr-2023	7.8	NVIDIA DGX-1 SBIOS contains a vulnerability in Bds, which may lead to code execution, denial of service, and escalation of privileges. **CVE ID : CVE-2023-25509**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	H-NVI-DGX--030523/596
Product: dgx-2					
Affected Version(s): -					
Out-of-bounds Write	22-Apr-2023	6.7	NVIDIA DGX-2 contains a vulnerability in OFBD where a user with high privileges and a pre-conditioned heap can cause an access beyond a buffers end, which may lead to code execution, escalation of privileges, denial of service, and	https://nvidia.custhelp.com/app/answers/detail/a_id/5449	H-NVI-DGX--030523/597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2023-0200**		
Out-of-bounds Write	22-Apr-2023	6.7	NVIDIA DGX-2 SBIOS contains a vulnerability in Bds, where a user with high privileges can cause a write beyond the bounds of an indexable resource, which may lead to code execution, denial of service, compromised integrity, and information disclosure. **CVE ID : CVE-2023-0201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5449	H-NVI-DGX--030523/598
Incorrect Permission Assignment for Critical Resource	22-Apr-2023	4.4	NVIDIA DGX-2 SBIOS contains a vulnerability where an attacker may modify the ServerSetup NVRAM variable at runtime by executing privileged code. A successful exploit of this vulnerability may lead to denial of service. **CVE ID : CVE-2023-0207**	https://nvidia.custhelp.com/app/answers/detail/a_id/5449	H-NVI-DGX--030523/599
Vendor: Phoenixcontact					
Product: infobox					
Affected Version(s): -					
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an	N/A	H-PHO-INFO-030523/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**		
Product: smartrtu_axc_ig					
Affected Version(s): -					
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**	N/A	H-PHO-SMAR-030523/601
Product: smartrtu_axc_sg					
Affected Version(s): -					
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an authenticated	N/A	H-PHO-SMAR-030523/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**		
Vendor: Schneider-electric					
Product: 140cpu65					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	H-SCH-140C-030523/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: bmeh58s					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**	N/A	H-SCH-BMEH-030523/604
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.	N/A	H-SCH-BMEH-030523/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25620		
Product: bmep58s					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**	N/A	H-SCH-BMEP-030523/606
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.	N/A	H-SCH-BMEP-030523/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25620		
Product: conext_gateway					
Affected Version(s): -					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	H-SCH-CONE-030523/608
Product: insightfacility					
Affected Version(s): -					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists	https://download.schneider-electric.com/files?p_Doc_	H-SCH-INSI-030523/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	
Product: insighthome					
Affected Version(s): -					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	H-SCH-INSI-030523/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29410		
Product: merten_instabus_tastermodul_1fach_system_m					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/611
Product: merten_instabus_tastermodul_2fach_system_m					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25556		
Product: merten_jalousie-\/schaltaktor_reg-k\/8x\/16x\/10_m._hb					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/613
Product: merten_knx_argus_180\/2\,20m_up_system					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25556		
Product: merten_knx_schaltakt.2x6a_up_m.2_eing.					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/615
Product: merten_knx_uni-dimmaktor_ll_reg-k\/2x230\/300_w					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25556		
Product: merten_tasterschnittstelle_4fach_plus					
Affected Version(s): -					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	H-SCH-MERT-030523/617
Product: modicon_m340					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.	N/A	H-SCH-MODI-030523/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25619		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	H-SCH-MODI-030523/619
Product: modicon_m580					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP	N/A	H-SCH-MODI-030523/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocol. **CVE ID : CVE-2023-25619**		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	H-SCH-MODI-030523/621
Product: modicon_mc80					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the	N/A	H-SCH-MODI-030523/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	H-SCH-MODI-030523/623
Product: modicon_momentum_unity_m1e_processor					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions	N/A	H-SCH-MODI-030523/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	H-SCH-MODI-030523/625
Product: powerlogic_hdpm6000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	18-Apr-2023	9.8	A CWE-129: Improper validation of an array index vulnerability exists where a specially crafted Ethernet request could result in denial of service or remote code execution. **CVE ID : CVE-2023-28004**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-02.pdf	H-SCH-POWE-030523/626
Product: tsxp57					
Affected Version(s): -					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.	N/A	H-SCH-TSXP-030523/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25619		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	H-SCH-TSXP-030523/628
Vendor: Tenda					
Product: ac15					
Affected Version(s): -					
Out-of-bounds Write	24-Apr-2023	9.8	Tenda AC15 V15.03.05.19 is vulnerable to Buffer Overflow. **CVE ID : CVE-2023-30369**	N/A	H-TEN-AC15-030523/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function GetValue contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30370**	N/A	H-TEN-AC15-030523/630
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "sub_ED14" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30371**	N/A	H-TEN-AC15-030523/631
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, The function "xkjs_ver32" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30372**	N/A	H-TEN-AC15-030523/632
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "xian_pppoe_user" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30373**	N/A	H-TEN-AC15-030523/633
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "getIfIp" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30375**	N/A	H-TEN-AC15-030523/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "henan_pppoe_user" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30376**	N/A	H-TEN-AC15-030523/635
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "sub_8EE8" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30378**	N/A	H-TEN-AC15-030523/636
Product: ac5					
Affected Version(s): -					
Out-of-bounds Write	24-Apr-2023	9.8	Tenda AC5 V15.03.06.28 is vulnerable to Buffer Overflow via the initWebs function. **CVE ID : CVE-2023-30368**	N/A	H-TEN-AC5-030523/637
Operating System					
Vendor: ami					
Product: megarac_sp-x					
Affected Version(s): 12					
Insufficient Verification of Data Authenticity	18-Apr-2023	9.1	AMI MegaRAC SPx12 and SPx13 devices have Insufficient Verification of Data Authenticity. **CVE ID : CVE-2023-28863**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023003.pdf	O-AMI-MEGA-030523/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 13					
Insufficient Verification of Data Authenticity	18-Apr-2023	9.1	AMI MegaRAC SPx12 and SPx13 devices have Insufficient Verification of Data Authenticity. **CVE ID : CVE-2023-28863**	https://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023003.pdf	O-AMI-MEGA-030523/639
Vendor: Apple					
Product: mac_os_x					
Affected Version(s): * Up to (including) 10.15					
Untrusted Search Path	18-Apr-2023	7	Qualys Cloud Agent for macOS (versions 2.5.1-75 before 3.7) installer allows a local escalation of privilege bounded only to the time of installation and only on older macOSX (macOS 10.15 and older) versions. Attackers may exploit incorrect file permissions to give them ROOT command execution privileges on the host. During the install of the PKG, a step in the process involves extracting the package and copying files to several directories. Attackers may gain writable	https://qualys.com/security-advisories	O-APP-MAC_-030523/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to files during the install of PKG when extraction of the package and copying files to several directories, enabling a local escalation of privilege. **CVE ID : CVE-2023-28143**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to	https://github.com/redis/redis/commit/bc7fe41e5857a0854d524e2a63a028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-hjv8-vjf6-wcr6,	O-DEB-DEBI-030523/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	https://github.com/redis/redis/pull/11149	
Affected Version(s): 11.0					
Integer Overflow or Wraparound	19-Apr-2023	9.6	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2136**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-DEB-DEBI-030523/642
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2133**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-DEB-DEBI-030523/643
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-	O-DEB-DEBI-030523/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2134**	desktop_18.html	
Out-of-bounds Write	19-Apr-2023	8.8	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2137**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-DEB-DEBI-030523/645
Use After Free	19-Apr-2023	7.5	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2135**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-DEB-DEBI-030523/646
Vendor: Dlink					
Product: dir-823g_firmware					
Affected Version(s): 1.0.2b05					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Apr-2023	9.8	D-Link DIR823G_V1.0.2B05 was discovered to contain a stack overflow via the NewPassword parameters in SetPasswdSettings. **CVE ID : CVE-2023-29665**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--030523/647
Vendor: electra-air					
Product: central_ac_unit_firmware					
Affected Version(s): v4					
Use of Hard-coded Credentials	17-Apr-2023	9.8	Electra Central AC unit – Hardcoded Credentials in unspecified code used by the unit. **CVE ID : CVE-2023-24501**	N/A	O-ELE-CENT-030523/648
Inadequate Encryption Strength	17-Apr-2023	6.5	Electra Central AC unit – The unit opens an AP with an easily calculated password. **CVE ID : CVE-2023-24502**	N/A	O-ELE-CENT-030523/649
Affected Version(s): v5					
Use of Hard-coded Credentials	17-Apr-2023	9.8	Electra Central AC unit – Hardcoded Credentials in unspecified code used by the unit. **CVE ID : CVE-2023-24501**	N/A	O-ELE-CENT-030523/650
Inadequate Encryption Strength	17-Apr-2023	6.5	Electra Central AC unit – The unit opens an AP with an easily calculated password.	N/A	O-ELE-CENT-030523/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24502		
Affected Version(s): v7					
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to load unauthorized FW. **CVE ID : CVE-2023-24500**	N/A	O-ELE-CENT-030523/652
Inadequate Encryption Strength	17-Apr-2023	6.5	Electra Central AC unit – The unit opens an AP with an easily calculated password. **CVE ID : CVE-2023-24502**	N/A	O-ELE-CENT-030523/653
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to connect to unauthorized update server. **CVE ID : CVE-2023-24504**	N/A	O-ELE-CENT-030523/654
Affected Version(s): v8					
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to load unauthorized FW. **CVE ID : CVE-2023-24500**	N/A	O-ELE-CENT-030523/655
Inadequate Encryption Strength	17-Apr-2023	6.5	Electra Central AC unit – The unit opens an AP with an easily calculated password. **CVE ID : CVE-2023-24502**	N/A	O-ELE-CENT-030523/656
N/A	17-Apr-2023	6.5	Electra Central AC unit – Adjacent attacker may cause the unit to connect to	N/A	O-ELE-CENT-030523/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update server. **CVE ID : CVE-2023-24504**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Integer Overflow or Wraparound	19-Apr-2023	9.6	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2136**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/658
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2133**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/659
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137	https://chromereleases.googleblog.com/2023/04/stable-	O-FED-FEDO-030523/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2134**	channel-update-for-desktop_18.html	
Out-of-bounds Write	19-Apr-2023	8.8	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2137**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/661
Use After Free	19-Apr-2023	7.5	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2135**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/662
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated	https://github.com/redis/redis/commit/bc7fe41	O-FED-FEDO-030523/663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	e5857a0854d524e2a63a028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-hjv8-vjf6-wcr6, https://github.com/redis/redis/pull/11149	
Affected Version(s): 37					
Integer Overflow or Wraparound	19-Apr-2023	9.6	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2136**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/664
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: High) **CVE ID : CVE-2023-2133**		
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2134**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/666
Out-of-bounds Write	19-Apr-2023	8.8	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2137**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/667
Use After Free	19-Apr-2023	7.5	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2135**		
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT` command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	https://github.com/redis/redis/commit/bc7fe41e5857a0854d524e2a63a028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-hjv8-vjf6-wcr6, https://github.com/redis/redis/pull/11149	O-FED-FEDO-030523/669
Affected Version(s): 38					
Integer Overflow or Wraparound	19-Apr-2023	9.6	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2136**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2133**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/671
Out-of-bounds Write	19-Apr-2023	8.8	Out of bounds memory access in Service Worker API in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2134**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/672
Out-of-bounds Write	19-Apr-2023	8.8	Heap buffer overflow in sqlite in Google Chrome prior to 112.0.5615.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2137**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Apr-2023	7.5	Use after free in DevTools in Google Chrome prior to 112.0.5615.137 allowed a remote attacker who convinced a user to enable specific preconditions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2135**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html	O-FED-FEDO-030523/674
Out-of-bounds Write	20-Apr-2023	6.7	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution. **CVE ID : CVE-2023-2194**	https://bugzilla.redhat.com/show_bug.cgi?id=2188396, https://github.com/torvalds/linux/commit/92fbb6d1296f	O-FED-FEDO-030523/675
Improper Input Validation	18-Apr-2023	6.5	Redis is an open source, in-memory database that persists on disk. Authenticated users can use the `HINCRBYFLOAT`	https://github.com/redis/redis/commit/bc7fe41e5857a0854d524e2a63a	O-FED-FEDO-030523/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command to create an invalid hash field that will crash Redis on access in affected versions. This issue has been addressed in in versions 7.0.11, 6.2.12, and 6.0.19. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2023-28856**	028e9394d2a5c, https://github.com/redis/redis/security/advisories/GHSA-hjv8-vjf6-wcr6, https://github.com/redis/redis/pull/11149	
Vendor: Google					
Product: android					
Affected Version(s): 11.0					
Out-of-bounds Write	19-Apr-2023	8.8	In nci_snd_set_routing_cmd of nci_hmsgs.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-264879662 **CVE ID : CVE-2023-21085**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	19-Apr-2023	7.8	In AlarmManagerActivity of AlarmManagerActivity.java, there is a possible way to bypass background activity launch restrictions via a pendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-195756028 **CVE ID : CVE-2023-20950**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/678
Out-of-bounds Write	19-Apr-2023	7.8	In avdt_scb_hdl_pkt_no_frag of avdt_scb_act.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-225879503 **CVE ID : CVE-2023-20967**		
N/A	19-Apr-2023	7.8	In multiple functions of PackageInstallerService.java and related files, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-230492955 **CVE ID : CVE-2023-21081**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/680
N/A	19-Apr-2023	7.8	In onNullBinding of CallScreeningServiceHelper.java, there is a possible way to record audio without showing a privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252762941 **CVE ID : CVE-2023-21083**		
N/A	19-Apr-2023	7.8	In isToggleable of SecureNfcEnabler.java and SecureNfcPreferenceController.java, there is a possible way to enable NFC from a secondary account due to a permissions bypass. This could lead to local escalation of privilege from the Guest account with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238298970 **CVE ID : CVE-2023-21086**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/682
N/A	19-Apr-2023	7.8	In startInstrumentation of ActivityManagerService.java, there is a possible way to keep the foreground service alive while the app is in the background. This could lead to	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237766679 **CVE ID : CVE-2023-21089**		
N/A	19-Apr-2023	7.8	In retrieveServiceLocked of ActiveServices.java, there is a possible way to dynamically register a BroadcastReceiver using permissions of System App due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242040055 **CVE ID : CVE-2023-21092**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/684
Improper Limitation of a Pathname	19-Apr-2023	7.8	In extractRelativePath of FileUtils.java, there is a possible way to access files in a	https://source.android.com/security	O-GOO-ANDR-030523/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			directory belonging to other applications due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-228450832 **CVE ID : CVE-2023-21093**	/bulletin/2023-04-01	
Missing Authorization	19-Apr-2023	7.8	In sanitize of LayerState.cpp, there is a possible way to take over the screen display and swap the display content due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-248031255 **CVE ID : CVE-2023-21094**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/686
Externally Controlled Reference	19-Apr-2023	7.8	In toUriInner of Intent.java, there is a possible way to launch	https://source.android.com/security	O-GOO-ANDR-030523/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Resource in Another Sphere			an arbitrary activity due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261858325 **CVE ID : CVE-2023-21097**	/bulletin/2023-04-01	
N/A	19-Apr-2023	7.8	In multiple functions of AccountManagerService.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260567867 **CVE ID : CVE-2023-21098**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/688
N/A	19-Apr-2023	7.8	In multiple methods of PackageInstallerSession.java, there is a	https://source.android.com/security	O-GOO-ANDR-030523/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible way to start foreground services from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243377226 **CVE ID : CVE-2023-21099**	/bulletin/2023-04-01	
N/A	19-Apr-2023	5.5	In multiple functions of RunningTasks.java, there is a possible privilege escalation due to a missing privilege check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243130512 **CVE ID : CVE-2023-20909**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	19-Apr-2023	5.5	In deserialize of multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-256589724 **CVE ID : CVE-2023-20935**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/691
Out-of-bounds Read	19-Apr-2023	5.5	In register_notification_rsp of btif_rc.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245916076 **CVE ID : CVE-2023-21080**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-2023	5.5	In getNumberFromCallIntent of NewOutgoingCallIntentBroadcaster.java, there is a possible way to enumerate other user's contact phone number due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-257030107 **CVE ID : CVE-2023-21082**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/693
N/A	19-Apr-2023	5.5	In PreferencesHelper.java, an uncaught exception may cause the device to get stuck in a boot loop. This could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261723753	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21087		
Affected Version(s): -					
Out-of-bounds Write	19-Apr-2023	6.6	In acc_ctrlrequest_composite of f_accessory.c, there is a possible out of bounds write due to a missing bounds check. This could lead to physical escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-264029575References: Upstream kernel **CVE ID : CVE-2023-20941**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/695
Affected Version(s): 12.0					
Use After Free	19-Apr-2023	9.8	In OnWakelockReleased of attribution_processor.cc, there is a use after free that could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13Android ID: A-254774758 **CVE ID : CVE-2023-21096**		
Out-of-bounds Write	19-Apr-2023	8.8	In nci_snd_set_routing_cmd of nci_hmsgs.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-264879662 **CVE ID : CVE-2023-21085**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/697
Incorrect Authorization	19-Apr-2023	7.8	In AlarmManagerActivity of AlarmManagerActivity.java, there is a possible way to bypass background activity launch restrictions via a pendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-195756028 **CVE ID : CVE-2023-20950**		
Out-of-bounds Write	19-Apr-2023	7.8	In avdt_scb_hdl_pkt_no_frag of avdt_scb_act.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225879503 **CVE ID : CVE-2023-20967**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/699
N/A	19-Apr-2023	7.8	In multiple functions of PackageInstallerService.java and related files, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-230492955 **CVE ID : CVE-2023-21081**		
N/A	19-Apr-2023	7.8	In onNullBinding of CallScreeningServiceHelper.java, there is a possible way to record audio without showing a privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252762941 **CVE ID : CVE-2023-21083**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/701
N/A	19-Apr-2023	7.8	In isToggleable of SecureNfcEnabler.java and SecureNfcPreferenceController.java, there is a possible way to enable NFC from a secondary account due to a permissions	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass. This could lead to local escalation of privilege from the Guest account with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238298970 **CVE ID : CVE-2023-21086**		
N/A	19-Apr-2023	7.8	In deliverOnFlushComplete of LocationProviderManager.java, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-235823542 **CVE ID : CVE-2023-21088**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-2023	7.8	In startInstrumentation of ActivityManagerService.java, there is a possible way to keep the foreground service alive while the app is in the background. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237766679 **CVE ID : CVE-2023-21089**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/704
N/A	19-Apr-2023	7.8	In retrieveServiceLocked of ActiveServices.java, there is a possible way to dynamically register a BroadcastReceiver using permissions of System App due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-242040055 **CVE ID : CVE-2023-21092**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Apr-2023	7.8	In extractRelativePath of FileUtils.java, there is a possible way to access files in a directory belonging to other applications due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-228450832 **CVE ID : CVE-2023-21093**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/706
Missing Authorization	19-Apr-2023	7.8	In sanitize of LayerState.cpp, there is a possible way to take over the screen display and swap the display content due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-248031255 **CVE ID : CVE-2023-21094**		
Externally Controlled Reference to a Resource in Another Sphere	19-Apr-2023	7.8	In toUriInner of Intent.java, there is a possible way to launch an arbitrary activity due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261858325 **CVE ID : CVE-2023-21097**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/708
N/A	19-Apr-2023	7.8	In multiple functions of AccountManagerService.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260567867 **CVE ID : CVE-2023-21098**		
N/A	19-Apr-2023	7.8	In multiple methods of PackageInstallerSession.java, there is a possible way to start foreground services from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243377226 **CVE ID : CVE-2023-21099**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/710
Out-of-bounds Write	19-Apr-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12L Android-13Android ID: A-242544249 **CVE ID : CVE-2023-21100**		
N/A	19-Apr-2023	5.5	In multiple functions of RunningTasks.java, there is a possible privilege escalation due to a missing privilege check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243130512 **CVE ID : CVE-2023-20909**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/712
Out-of-bounds Read	19-Apr-2023	5.5	In deserialize of multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-256589724 **CVE ID : CVE-2023-20935**		
Out-of-bounds Read	19-Apr-2023	5.5	In register_notification_rsp of btif_rc.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245916076 **CVE ID : CVE-2023-21080**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/714
N/A	19-Apr-2023	5.5	In getNumberFromCallIntent of NewOutgoingCallIntentBroadcaster.java, there is a possible way to enumerate other user's contact phone number due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-257030107 **CVE ID : CVE-2023-21082**		
N/A	19-Apr-2023	5.5	In PreferencesHelper.java, an uncaught exception may cause the device to get stuck in a boot loop. This could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261723753 **CVE ID : CVE-2023-21087**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/716
Affected Version(s): 12.1					
Use After Free	19-Apr-2023	9.8	In OnWakelockReleased of attribution_processor.cc, there is a use after free that could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12L Android-13Android ID: A-254774758 **CVE ID : CVE-2023-21096**		
Out-of-bounds Write	19-Apr-2023	8.8	In nci_snd_set_routing_cmd of nci_hmsgs.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-264879662 **CVE ID : CVE-2023-21085**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/718
Incorrect Authorization	19-Apr-2023	7.8	In AlarmManagerActivity of AlarmManagerActivity.java, there is a possible way to bypass background activity launch restrictions via a pendingIntent. This could lead to local escalation of privilege with no additional execution privileges	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-195756028 **CVE ID : CVE-2023-20950**		
Out-of-bounds Write	19-Apr-2023	7.8	In avdt_scb_hdl_pkt_no_frag of avdt_scb_act.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225879503 **CVE ID : CVE-2023-20967**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/720
N/A	19-Apr-2023	7.8	In multiple functions of PackageInstallerService.java and related files, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-230492955 **CVE ID : CVE-2023-21081**		
N/A	19-Apr-2023	7.8	In onNullBinding of CallScreeningServiceHelper.java, there is a possible way to record audio without showing a privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252762941 **CVE ID : CVE-2023-21083**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/722
N/A	19-Apr-2023	7.8	In isToggleable of SecureNfcEnabler.java and SecureNfcPreferenceController.java, there is a possible way to enable NFC from a	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			secondary account due to a permissions bypass. This could lead to local escalation of privilege from the Guest account with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238298970 **CVE ID : CVE-2023-21086**		
N/A	19-Apr-2023	7.8	In deliverOnFlushComplete of LocationProviderManager.java, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-235823542 **CVE ID : CVE-2023-21088**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-2023	7.8	In startInstrumentation of ActivityManagerService.java, there is a possible way to keep the foreground service alive while the app is in the background. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237766679 **CVE ID : CVE-2023-21089**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/725
N/A	19-Apr-2023	7.8	In retrieveServiceLocked of ActiveServices.java, there is a possible way to dynamically register a BroadcastReceiver using permissions of System App due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-242040055 **CVE ID : CVE-2023-21092**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Apr-2023	7.8	In extractRelativePath of FileUtils.java, there is a possible way to access files in a directory belonging to other applications due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-228450832 **CVE ID : CVE-2023-21093**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/727
Missing Authorization	19-Apr-2023	7.8	In sanitize of LayerState.cpp, there is a possible way to take over the screen display and swap the display content due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-248031255 **CVE ID : CVE-2023-21094**		
Externally Controlled Reference to a Resource in Another Sphere	19-Apr-2023	7.8	In toUriInner of Intent.java, there is a possible way to launch an arbitrary activity due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261858325 **CVE ID : CVE-2023-21097**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/729
N/A	19-Apr-2023	7.8	In multiple functions of AccountManagerService.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260567867 **CVE ID : CVE-2023-21098**		
N/A	19-Apr-2023	7.8	In multiple methods of PackageInstallerSession.java, there is a possible way to start foreground services from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243377226 **CVE ID : CVE-2023-21099**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/731
Out-of-bounds Write	19-Apr-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12L Android-13Android ID: A-242544249 **CVE ID : CVE-2023-21100**		
N/A	19-Apr-2023	5.5	In multiple functions of RunningTasks.java, there is a possible privilege escalation due to a missing privilege check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243130512 **CVE ID : CVE-2023-20909**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/733
Out-of-bounds Read	19-Apr-2023	5.5	In deserialize of multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-256589724 **CVE ID : CVE-2023-20935**		
Out-of-bounds Read	19-Apr-2023	5.5	In register_notification_rsp of btif_rc.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245916076 **CVE ID : CVE-2023-21080**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/735
N/A	19-Apr-2023	5.5	In getNumberFromCallIntent of NewOutgoingCallIntentBroadcaster.java, there is a possible way to enumerate other user's contact phone number due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-257030107 **CVE ID : CVE-2023-21082**		
N/A	19-Apr-2023	5.5	In PreferencesHelper.java, an uncaught exception may cause the device to get stuck in a boot loop. This could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261723753 **CVE ID : CVE-2023-21087**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/737
Affected Version(s): 13.0					
Use After Free	19-Apr-2023	9.8	In OnWakelockReleased of attribution_processor.cc, there is a use after free that could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12 Android-12L Android-13Android ID: A-254774758 **CVE ID : CVE-2023-21096**		
Out-of-bounds Write	19-Apr-2023	8.8	In nci_snd_set_routing_cmd of nci_hmsgs.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-264879662 **CVE ID : CVE-2023-21085**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/739
Out-of-bounds Write	19-Apr-2023	7.8	In avdt_scb_hdl_pkt_no_frag of avdt_scb_act.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-225879503 **CVE ID : CVE-2023-20967**		
N/A	19-Apr-2023	7.8	In multiple functions of PackageInstallerService.java and related files, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-230492955 **CVE ID : CVE-2023-21081**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/741
N/A	19-Apr-2023	7.8	In onNullBinding of CallScreeningServiceHelper.java, there is a possible way to record audio without showing a privacy indicator due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252762941 **CVE ID : CVE-2023-21083**		
N/A	19-Apr-2023	7.8	In isToggleable of SecureNfcEnabler.java and SecureNfcPreferenceController.java, there is a possible way to enable NFC from a secondary account due to a permissions bypass. This could lead to local escalation of privilege from the Guest account with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-238298970 **CVE ID : CVE-2023-21086**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/743
N/A	19-Apr-2023	7.8	In deliverOnFlushComplete of LocationProviderManager.java, there is a possible way to bypass background	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-235823542 **CVE ID : CVE-2023-21088**		
N/A	19-Apr-2023	7.8	In startInstrumentation of ActivityManagerService.java, there is a possible way to keep the foreground service alive while the app is in the background. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-237766679 **CVE ID : CVE-2023-21089**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Apr-2023	7.8	In retrieveServiceLocked of ActiveServices.java, there is a possible way to dynamically register a BroadcastReceiver using permissions of System App due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-242040055 **CVE ID : CVE-2023-21092**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/746
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Apr-2023	7.8	In extractRelativePath of FileUtils.java, there is a possible way to access files in a directory belonging to other applications due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-228450832 **CVE ID : CVE-2023-21093**		
Missing Authorization	19-Apr-2023	7.8	In sanitize of LayerState.cpp, there is a possible way to take over the screen display and swap the display content due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-248031255 **CVE ID : CVE-2023-21094**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/748
Externally Controlled Reference to a Resource in Another Sphere	19-Apr-2023	7.8	In toUriInner of Intent.java, there is a possible way to launch an arbitrary activity due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-261858325 **CVE ID : CVE-2023-21097**		
N/A	19-Apr-2023	7.8	In multiple functions of AccountManagerService.java, there is a possible loading of arbitrary code into the System Settings app due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260567867 **CVE ID : CVE-2023-21098**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/750
N/A	19-Apr-2023	7.8	In multiple methods of PackageInstallerSession.java, there is a possible way to start foreground services from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-11 Android-12 Android-12L Android-13Android ID: A-243377226 **CVE ID : CVE-2023-21099**		
Out-of-bounds Write	19-Apr-2023	7.8	In inflate of inflate.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12L Android-13Android ID: A-242544249 **CVE ID : CVE-2023-21100**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/752
N/A	19-Apr-2023	6.7	In buildPropFile of filesystem.go, there is a possible insecure hash due to an improperly used crypto. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-262892300	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-21084		
N/A	19-Apr-2023	5.5	In multiple functions of RunningTasks.java, there is a possible privilege escalation due to a missing privilege check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-243130512 **CVE ID : CVE-2023-20909**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/754
Out-of-bounds Read	19-Apr-2023	5.5	In deserialize of multiple files, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-256589724	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20935		
Out-of-bounds Read	19-Apr-2023	5.5	In register_notification_rsp of btif_rc.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-245916076 **CVE ID : CVE-2023-21080**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/756
N/A	19-Apr-2023	5.5	In getNumberFromCallIntent of NewOutgoingCallIntentBroadcaster.java, there is a possible way to enumerate other user's contact phone number due to a confused deputy. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-257030107 **CVE ID : CVE-2023-21082**		
N/A	19-Apr-2023	5.5	In PreferencesHelper.java, an uncaught exception may cause the device to get stuck in a boot loop. This could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261723753 **CVE ID : CVE-2023-21087**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/758
Missing Authorization	19-Apr-2023	5.5	In canDisplayLocalUi of AppLocalePickerActivity.java, there is a possible way to change system app locales due to a missing permission check. This could lead to local denial of service across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-257954050 **CVE ID : CVE-2023-21091**		
Uncontrolled Resource Consumption	19-Apr-2023	5	In parseUsesPermission of ParsingPackageUtils.java, there is a possible boot loop due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-259942609 **CVE ID : CVE-2023-21090**	https://source.android.com/security/bulletin/2023-04-01	O-GOO-ANDR-030523/760
Vendor: Juniper					
Product: junos					
Affected Version(s): * Up to (excluding) 18.1					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): * Up to (excluding) 19.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_C		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Affected Version(s): * Up to (excluding) 19.3					
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Affected Version(s): * Up to (excluding) 19.4					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions;	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3;	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): * Up to (excluding) 20.2					
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_pr	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			epare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			D: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Affected Version(s): * Up to (excluding) 21.2					
Improper Handling of Exceptiona	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28970		
Affected Version(s): 18.1					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 18.2					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 18.3					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based,	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 18.4					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 19.1					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated,	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application:	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Affected Version(s): 19.2					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Affected Version(s): 19.3					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Improper Link Resolution Before File	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Affected Version(s): 19.4					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28964		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptiona	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28959		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the	https://supportportal.jun	O-JUN-JUNO-030523/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2.	iper.net/JSA70600	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28975		
Affected Version(s): 20.1					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28962		
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Affected Version(s): 20.2					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_C		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			M_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled:	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 20.3					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 20.4					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILE	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			D: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-	https://supportportal.jun	O-JUN-JUNO-030523/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.	iper.net/JSA 70587	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28963		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 21.1					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_IN		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			T_EVENTS_ENQ_192K _VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM ERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 21.2					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28972		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CM		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash,	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28974		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS:	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28968		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 21.3					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Link	17-Apr-2023	6.8	An Improper Link Resolution Before File	https://supportportal.jun	O-JUN-JUNO-030523/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resolution Before File Access ('Link Following')			Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to	iper.net/JSA70596	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/P		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			E_Chip/0/PECHIP_CM ERROR_CM_INT_REG_ DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Handling of Exceptiona l Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks	https://supp ortportal.jun iper.net/JSA 70594	O-JUN-JUNO-030523/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Improper Check for	17-Apr-2023	6.5	An Improper Check for Unusual or	https://supportportal.jun	O-JUN-JUNO-030523/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3	iper.net/JSA70599	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 21.4					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS:	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	7.5	An Improper Check or Handling of Exceptional Conditions within the storm control feature of Juniper Networks Junos OS allows an attacker sending a high rate of traffic to cause a Denial of Service. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. Storm control	https://supportportal.juniper.net/JSA70589	O-JUN-JUNO-030523/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			monitors the level of applicable incoming traffic and compares it with the level specified. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2. **CVE ID : CVE-2023-28965**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the	https://supportportal.jun	O-JUN-JUNO-030523/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2.	iper.net/JSA 70612	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1697		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end :		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 22.1					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Link Resolution Before File Access ('Link Following')	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series, PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
N/A	17-Apr-2023	5.3	An Improper Handling of Unexpected Data Type vulnerability in IPv6 firewall filter processing of Juniper Networks Junos OS on the ACX Series devices will prevent a firewall filter with the term 'from next-header ah' from being properly installed in the packet forwarding engine (PFE). There is no immediate indication of an incomplete firewall filter commit shown at the CLI, which could allow an attacker to send valid packets to or through the device that were explicitly intended to be dropped. An indication that the filter was not installed can be identified with the following logs: fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_rule_prepare : Config failed: Unsupported Ip-protocol 51 in the filter lo0.0-inet6-i fpc0 ACX_DFW_CFG_FAILE	https://supportportal.juniper.net/JSA70586	O-JUN-JUNO-030523/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			D: ACX Error (dfw):dnx_dfw_rule_prepare : Please detach the filter, remove unsupported match and re-attach fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_rule : Status:104 dnx_dfw_rule_prepare failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_process_filter : Status:104 dnx_dfw_process_rule failed fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_filter_in_hw : Status:104 Could not process filter(lo0.0-inet6-i) for rule expansion Unsupported match, action present. fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_create_hw_instance : Status:104 Could not program dfw(lo0.0-inet6-i) type(IFP_DFLT_INET6_Lo0_FILTER)! [104] fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_bind_shim : [104] Could not create dfw(lo0.0-inet6-i)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			type(IFP_DFLT_INET6_Lo0_FILTER) fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_update_resolve : [100] Failed to bind filter(3) to bind point fpc0 ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_change_end : dnx_dfw_update_resolve (resolve type) failed This issue affects Juniper Networks Junos OS on ACX Series: All versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. **CVE ID : CVE-2023-28961**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 22.2					
Unrestricted Upload of File with Dangerous Type	17-Apr-2023	9.8	An Improper Authentication vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Link Resolution Before File	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in console port access of	https://supportportal.juniper.net/JSA70596	O-JUN-JUNO-030523/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
N/A	17-Apr-2023	6.5	An Improper Handling of Missing Values vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a dcpfe process core and thereby a Denial of Service (DoS). Continued receipt of these specific frames will cause a sustained Denial of Service condition. This issue occurs when a specific malformed ethernet frame is received. This issue affects Juniper Networks Junos OS on QFX10000 Series,	https://supportportal.juniper.net/JSA70612	O-JUN-JUNO-030523/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PTX1000 Series Series: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2. **CVE ID : CVE-2023-1697**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Improper Check for Unusual or Exceptiona	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 22.3					
Unrestricted Upload of	17-Apr-2023	9.8	An Improper Authentication	https://supportportal.jun	O-JUN-JUNO-030523/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			vulnerability in upload-file.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to upload arbitrary files to temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to 20.4R3-S6; 21.1 version 21.1R1 and later versions; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28962**	iper.net/JSA70587	
Improper Link Resolution	17-Apr-2023	6.8	An Improper Link Resolution Before File Access vulnerability in	https://supportportal.jun	O-JUN-JUNO-030523/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Before File Access ('Link Following')			console port access of Juniper Networks Junos OS on NFX Series allows an attacker to bypass console access controls. When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on NFX Series systems, leading to a possible administrative bypass with physical access to the console. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. This is similar to the vulnerability described in CVE-2019-0035 but affects different platforms and in turn requires a different fix. This issue affects Juniper Networks Junos OS on NFX Series: 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S12; 20.2	iper.net/JSA70596	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.2R3-S8; 20.4 versions prior to 20.4R3-S7; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28972**		
Improper Check or Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on QFX10002 allows an unauthenticated, adjacent attacker on the local broadcast domain sending a malformed packet to the device, causing all PFEs other than the inbound PFE to wedge and to eventually restart, resulting in a Denial of Service (DoS) condition. Continued receipt and processing of this packet will create a	https://supportportal.juniper.net/JSA70584	O-JUN-JUNO-030523/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sustained Denial of Service (DoS) condition. This issue can only be triggered by sending a specific malformed packet to the device. Transit traffic does not trigger this issue. An indication of this issue occurring can be seen through the following log messages: fpc0 expr_hostbound_packet_handler: Receive pe 73? fpc0 Cmerror Op Set: PE Chip: PE0[0]: PGQ:misc_intr: 0x00000020: Enqueue of a packet with out-of-range VOQ in 192K-VOQ mode (URI: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL) The logs list below can also be observed when this issue occurs fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107), scope: pfe, category: functional, severity: major, module: PE Chip, type: Description for PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL fpc0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_PGQ_MISC_INT_EVENTS_ENQ_192K_VIOL (0x210107) in module: PE Chip with scope: pfe category: functional level: major fpc0 Error: /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a), scope: pfe, category: functional, severity: fatal, module: PE Chip, type: Description for PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE fpc0 Performing action cmalarm for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal fpc0 Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/PE_Chip/0/PECHIP_CMERROR_CM_INT_REG_DCHK_PIPE (0x21011a) in module: PE Chip with scope: pfe category: functional level: fatal		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects Juniper Networks Junos OS on QFX10002: All versions prior to 19.1R3-S10; 19.4 versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28959**		
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	6.5	An Improper Check for Unusual or Exceptional Conditions vulnerability in the bbe-smgd of Juniper Networks Junos OS allows an unauthenticated,	https://supportportal.juniper.net/JSA70599	O-JUN-JUNO-030523/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to cause a Denial of Service (DoS). In a Broadband Edge / Subscriber Management scenario on MX Series when a specifically malformed ICMP packet addressed to the device is received from a subscriber the bbe-smgd will crash, affecting the subscriber sessions that are connecting, updating, or terminating. Continued receipt of such packets will lead to a sustained DoS condition. When this issue happens the below log can be seen if the traceoptions for the processes smg-service are enabled: BBE_TRACE(TRACE_LEVEL_INFO, "%s: Dropped unsupported ICMP PKT ... This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 19.4R3-S11; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28974**		
Improper Authentication	17-Apr-2023	5.3	An Improper Authentication vulnerability in cert-mgmt.php, used by the J-Web component of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to read arbitrary files from temporary folders on the device. This issue affects Juniper Networks Junos OS: All versions prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions; 20.4 versions prior to	https://supportportal.juniper.net/JSA70587	O-JUN-JUNO-030523/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2. **CVE ID : CVE-2023-28963**		
Allocation of Resources Without Limits or Throttling	17-Apr-2023	5.3	An Improperly Controlled Sequential Memory Allocation vulnerability in the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) Application Signature component of Junos OS's AppID service on SRX Series devices will stop the JDPI-Decoder from identifying dynamic application traffic, allowing an unauthenticated network-based attacker to send traffic to the target device using the JDPI-Decoder, designed to inspect dynamic application traffic and take action upon this traffic, to instead	https://supportportal.juniper.net/JSA70592	O-JUN-JUNO-030523/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			begin to not take action and to pass the traffic through. An example session can be seen by running the following command and evaluating the output. user@device# run show security flow session source-prefix <address/mask> extensive Session ID: <session ID>, Status: Normal, State: Active Policy name: <name of policy> Dynamic application: junos:UNKNOWN, <<<<< LOOK HERE Please note, the JDPI-Decoder and the AppID SigPack are both affected and both must be upgraded along with the operating system to address the matter. By default, none of this is auto-enabled for automatic updates. This issue affects: Juniper Networks any version of the JDPI-Decoder Engine prior to version 5.7.0-47 with the JDPI-Decoder enabled using any version of the AppID SigPack prior to version 1.550.2-31 (SigPack 3533) on Junos OS on SRX Series: All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.1R3-S10; 19.2 versions prior to 19.2R3-S7; 19.3 versions prior to 19.3R3-S8; 19.4 versions prior to 19.4R3-S11; 20.1 version 20.1R1 and later versions prior to 20.2R3-S7; 20.3 version 20.3R1 and later versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S1, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; **CVE ID : CVE-2023-28968**		
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Affected Version(s): 22.4					
Improper Handling of Exceptional Conditions	17-Apr-2023	6.5	An Improper Check or Handling of Exceptional Conditions vulnerability in packet processing on the network interfaces of	https://supportportal.juniper.net/JSA70594	O-JUN-JUNO-030523/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on JRR200 route reflector appliances allows an adjacent, network-based attacker sending a specific packet to the device to cause a kernel crash, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue can only be triggered by an attacker on the local broadcast domain. Packets routed to the device are unable to trigger this crash. This issue affects Juniper Networks Junos OS on JRR200: All versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S4; 21.4 versions prior to 21.4R3-S3; 22.1 versions prior to 22.1R3-S1; 22.2 versions prior to 22.2R2-S2, 22.2R3; 22.3 versions prior to 22.3R1-S2, 22.3R2; 22.4 versions prior to 22.4R1-S1, 22.4R2. **CVE ID : CVE-2023-28970**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	17-Apr-2023	4.6	An Unexpected Status Code or Return Value vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated attacker with physical access to the device to cause a Denial of Service (DoS). When certain USB devices are connected to a USB port of the routing-engine (RE), the kernel will crash leading to a reboot of the device. The device will continue to crash as long as the USB device is connected. This issue affects Juniper Networks Junos OS: All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S7; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S4; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2, 22.2R3; 22.3 versions prior to	https://supportportal.juniper.net/JSA70600	O-JUN-JUNO-030523/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.3R1-S1, 22.3R2; 22.4 versions prior to 22.4R2. **CVE ID : CVE-2023-28975**		
Product: junos_os_evolved					
Affected Version(s): 20.1					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 20.2					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 20.3					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter Inconsistency vulnerability in the routing protocol daemon (rpd) of	https://supportportal.juniper.net/JSA70588	O-JUN-JUNO-030523/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): 20.4					
Incorrect Permission Assignment for Critical Resource	17-Apr-2023	8.2	An Incorrect Permission Assignment for Critical Resource vulnerability in Juniper Networks Junos OS Evolved allows a local, authenticated low-privileged attacker to copy potentially malicious files into an existing Docker container on the local system. A follow-on administrator could then inadvertently start the Docker container leading to the malicious files being executed as root. This issue only affects systems with Docker configured and enabled, which is not enabled by default. Systems without Docker started are not vulnerable to this issue. This issue affects Juniper Networks Junos OS Evolved: 20.4 versions prior to 20.4R3-S5-EVO; 21.2 versions	https://supportportal.juniper.net/JSA70585	O-JUN-JUNO-030523/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.2R3-EVO; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2023-28960**		
Incorrect Default Permissions	17-Apr-2023	7.8	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS Evolved allows a low-privileged local attacker with shell access to modify existing files or execute commands as root. The issue is caused by improper file and directory permissions on certain system files, allowing an attacker with access to these files and folders to inject CLI commands as root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO. **CVE ID : CVE-2023-28966**	https://supportportal.juniper.net/JSA70590	O-JUN-JUNO-030523/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Apr-2023	7.1	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO.	https://supportportal.juniper.net/JSA70597	O-JUN-JUNO-030523/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28973		
Affected Version(s): 21.1					
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Authentication	17-Apr-2023	7.1	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of	https://supportportal.juniper.net/JSA70597	O-JUN-JUNO-030523/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO. **CVE ID : CVE-2023-28973**		
Affected Version(s): 21.2					
Incorrect Permission Assignment for Critical Resource	17-Apr-2023	8.2	An Incorrect Permission Assignment for Critical Resource vulnerability in Juniper Networks Junos OS Evolved allows a local, authenticated low-	https://supportportal.juniper.net/JSA70585	O-JUN-JUNO-030523/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker to copy potentially malicious files into an existing Docker container on the local system. A follow-on administrator could then inadvertently start the Docker container leading to the malicious files being executed as root. This issue only affects systems with Docker configured and enabled, which is not enabled by default. Systems without Docker started are not vulnerable to this issue. This issue affects Juniper Networks Junos OS Evolved: 20.4 versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2023-28960**		
Incorrect Default Permissions	17-Apr-2023	7.8	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS Evolved	https://supportportal.juniper.net/JSA70590	O-JUN-JUNO-030523/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a low-privileged local attacker with shell access to modify existing files or execute commands as root. The issue is caused by improper file and directory permissions on certain system files, allowing an attacker with access to these files and folders to inject CLI commands as root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO. **CVE ID : CVE-2023-28966**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Authentication	17-Apr-2023	7.1	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper	https://supportportal.juniper.net/JSA70597	O-JUN-JUNO-030523/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO. **CVE ID : CVE-2023-28973**		
Affected Version(s): 21.3					
Incorrect Permission Assignment for Critical Resource	17-Apr-2023	8.2	An Incorrect Permission Assignment for Critical Resource vulnerability in Juniper Networks Junos OS Evolved allows a local, authenticated low-privileged attacker to copy potentially malicious files into an existing Docker container on the local system. A follow-on administrator could then inadvertently start the Docker container leading to the malicious files being executed as root. This issue only affects systems with Docker configured and enabled, which is not enabled by default. Systems without Docker started are not vulnerable to this issue. This issue	https://supportportal.juniper.net/JSA70585	O-JUN-JUNO-030523/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS Evolved: 20.4 versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2023-28960**		
Incorrect Default Permissions	17-Apr-2023	7.8	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS Evolved allows a low-privileged local attacker with shell access to modify existing files or execute commands as root. The issue is caused by improper file and directory permissions on certain system files, allowing an attacker with access to these files and folders to inject CLI commands as root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions	https://supportportal.juniper.net/JSA70590	O-JUN-JUNO-030523/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO. **CVE ID : CVE-2023-28966**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Authentication	17-Apr-2023	7.1	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative	https://supportportal.juniper.net/JSA70597	O-JUN-JUNO-030523/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO. **CVE ID : CVE-2023-28973**		
Affected Version(s): 21.4					
Incorrect Permission Assignment for Critical Resource	17-Apr-2023	8.2	An Incorrect Permission Assignment for Critical Resource vulnerability in Juniper Networks Junos OS Evolved	https://supportportal.juniper.net/JSA70585	O-JUN-JUNO-030523/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a local, authenticated low-privileged attacker to copy potentially malicious files into an existing Docker container on the local system. A follow-on administrator could then inadvertently start the Docker container leading to the malicious files being executed as root. This issue only affects systems with Docker configured and enabled, which is not enabled by default. Systems without Docker started are not vulnerable to this issue. This issue affects Juniper Networks Junos OS Evolved: 20.4 versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2023-28960**		
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway	https://supportportal.jun	O-JUN-JUNO-030523/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions	iper.net/JSA70591	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Improper Authentication	17-Apr-2023	7.1	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node	https://supportportal.juniper.net/JSA70597	O-JUN-JUNO-030523/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to 21.4R1-S2-EVO, 21.4R2-EVO. **CVE ID : CVE-2023-28973**		
Affected Version(s): 22.1					
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO;		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Affected Version(s): 22.2					
Use of Uninitialized Resource	17-Apr-2023	7.5	A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is	https://supportportal.juniper.net/JSA70591	O-JUN-JUNO-030523/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO. **CVE ID : CVE-2023-28967**		
Affected Version(s): * Up to (excluding) 20.1					
N/A	17-Apr-2023	7.5	An Improper Handling of Length Parameter	https://supportportal.jun	O-JUN-JUNO-030523/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Inconsistency vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network based, unauthenticated attacker to cause an RPD crash leading to a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. Upon receipt of a malformed BGP flowspec update, RPD will crash resulting in a Denial of Service. This issue affects Juniper Networks Junos OS: All versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions	iper.net/JSA 70588	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.3R1-S1, 20.3R2; Juniper Networks Junos OS Evolved: All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO; 20.3 versions prior to 20.3R2-EVO; **CVE ID : CVE-2023-28964**		
Affected Version(s): * Up to (excluding) 20.4					
Incorrect Default Permissions	17-Apr-2023	7.8	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS Evolved allows a low-privileged local attacker with shell access to modify existing files or execute commands as root. The issue is caused by improper file and directory permissions on certain system files, allowing an attacker with access to these files and folders to inject CLI commands as root. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO.	https://supportportal.juniper.net/JSA70590	O-JUN-JUNO-030523/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28966		
Improper Authentication	17-Apr-2023	7.1	An Improper Authorization vulnerability in the 'sysmanctl' shell command of Juniper Networks Junos OS Evolved allows a local, authenticated attacker to execute administrative commands that could impact the integrity of the system or system availability. Administrative functions such as daemon restarting, routing engine (RE) switchover, and node shutdown can all be performed through exploitation of the 'sysmanctl' command. Access to the 'sysmanctl' command is only available from the Junos shell. Neither direct nor indirect access to 'sysmanctl' is available from the Junos CLI. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S5-EVO; 21.2 versions prior to 21.2R3-EVO; 21.3 versions prior to 21.3R2-EVO; 21.4 versions prior to	https://supportportal.juniper.net/JSA70597	O-JUN-JUNO-030523/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			21.4R1-S2-EVO, 21.4R2-EVO. **CVE ID : CVE-2023-28973**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 5.19					
NULL Pointer Dereference	20-Apr-2023	5.5	A null pointer dereference issue was found in the sctp network protocol in net/sctp/stream_sched.c in Linux Kernel. If stream_in allocation is failed, stream_out is freed which would further be accessed. A local user could use this flaw to crash the system or potentially cause a denial of service. **CVE ID : CVE-2023-2177**	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=181d8d2066c0	O-LIN-LINU-030523/929
Affected Version(s): * Up to (excluding) 6.0					
NULL Pointer Dereference	19-Apr-2023	5.5	A NULL pointer dereference flaw was found in the UNIX protocol in net/unix/diag.c In unix_diag_get_exact in the Linux Kernel. The newly allocated skb does not have sk, leading to a NULL pointer. This flaw allows a local user to crash or potentially cause a denial of service.	https://bugzilla.redhat.com/show_bug.cgi?id=2177382	O-LIN-LINU-030523/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28327		
Affected Version(s): * Up to (excluding) 6.1					
NULL Pointer Dereference	19-Apr-2023	5.5	A null pointer dereference issue was found in can protocol in net/can/af_can.c in the Linux before Linux. ml_priv may not be initialized in the receive path of CAN frames. A local user could use this flaw to crash the system or potentially cause a denial of service. **CVE ID : CVE-2023-2166**	https://lore.kernel.org/lkml/CAO4mrfcV_07hbj8NUuZrA8FH-kaRsrFy-2metecpTuE5kKHn5w@mail.gmail.com/	O-LIN-LINU-030523/931
NULL Pointer Dereference	19-Apr-2023	4.7	A data race flaw was found in the Linux kernel, between where con is allocated and con->sock is set. This issue leads to a NULL pointer dereference when accessing con->sock->sk in net/tipc/topsrv.c in the tipc protocol in the Linux kernel. **CVE ID : CVE-2023-1382**	https://lore.kernel.org/netdev/bc7bd3183f1c275c820690fc65b708238fe9e38e.1668807842.git.lucien.xin@gmail.com/T/#u	O-LIN-LINU-030523/932
Affected Version(s): * Up to (excluding) 6.2					
Use After Free	19-Apr-2023	5.5	A use-after-free vulnerability was found in iscsi_sw_tcp_session_create in drivers/scsi/iscsi_tcp.c in SCSI sub-	https://www.spinics.net/lists/linux-scsi/msg181542.html	O-LIN-LINU-030523/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component in the Linux Kernel. In this flaw an attacker could leak kernel internal information. **CVE ID : CVE-2023-2162**		
NULL Pointer Dereference	19-Apr-2023	5.5	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Linux Kernel. The message from user space is not checked properly before transferring into the device. This flaw allows a local user to crash the system or potentially cause a denial of service. **CVE ID : CVE-2023-28328**	https://bugzilla.redhat.com/show_bug.cgi?id=2177389	O-LIN-LINU-030523/934
Affected Version(s): * Up to (excluding) 6.2.9					
Use After Free	16-Apr-2023	6.4	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/power/supply/da9150-charger.c if a physically proximate attacker unplugs a device. **CVE ID : CVE-2023-30772**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=06615d11cc78162dfd5116efb71f29eb29502d37, https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-	O-LIN-LINU-030523/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				6.2.9, https://bugzilla.suse.com/show_bug.cgi?id=1210329	
Affected Version(s): * Up to (excluding) 6.3					
Out-of-bounds Write	20-Apr-2023	6.7	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution. **CVE ID : CVE-2023-2194**	https://bugzilla.redhat.com/show_bug.cgi?id=2188396, https://github.com/torvalds/linux/commit/92fbb6d1296f	O-LIN-LINU-030523/936
Affected Version(s): 5.19					
NULL Pointer Dereference	20-Apr-2023	5.5	A null pointer dereference issue was found in the sctp network protocol in net/sctp/stream_sched.c in Linux Kernel. If stream_in allocation is failed, stream_out is freed which would further be accessed. A local user could use this flaw to crash the system or potentially	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=181d8d2066c0	O-LIN-LINU-030523/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service. **CVE ID : CVE-2023-2177**		
Affected Version(s): 6.1					
NULL Pointer Dereference	19-Apr-2023	5.5	A null pointer dereference issue was found in can protocol in net/can/af_can.c in the Linux before Linux. ml_priv may not be initialized in the receive path of CAN frames. A local user could use this flaw to crash the system or potentially cause a denial of service. **CVE ID : CVE-2023-2166**	https://lore.kernel.org/lkml/CAO4mrfcV_07hbj8NUuZrA8FH-kaRsrFy-2metecpTuE5kKHn5w@mail.gmail.com/	O-LIN-LINU-030523/938
NULL Pointer Dereference	19-Apr-2023	4.7	A data race flaw was found in the Linux kernel, between where con is allocated and con->sock is set. This issue leads to a NULL pointer dereference when accessing con->sock->sk in net/tipc/topsrv.c in the tipc protocol in the Linux kernel. **CVE ID : CVE-2023-1382**	https://lore.kernel.org/netdev/bc7bd3183f1c275c820690fc65b708238fe9e38e.1668807842.git.lucien.xin@gmail.com/T/#u	O-LIN-LINU-030523/939
Affected Version(s): 6.2					
Use After Free	19-Apr-2023	5.5	A use-after-free vulnerability was found in iscsi_sw_tcp_session_c	https://www.spinics.net/lists/linux-	O-LIN-LINU-030523/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reate in drivers/scsi/iscsi_tcp.c in SCSI sub-component in the Linux Kernel. In this flaw an attacker could leak kernel internal information. **CVE ID : CVE-2023-2162**	scsi/msg18154 2.html	
Affected Version(s): 6.3					
Out-of-bounds Write	20-Apr-2023	6.7	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution. **CVE ID : CVE-2023-2194**	https://bugzilla.redhat.com/show_bug.cgi?id=2188396, https://github.com/torvalds/linux/commit/92fbb6d1296f	O-LIN-LINU-030523/941
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
NULL Pointer Dereference	19-Apr-2023	5.5	Avast and AVG Antivirus for Windows were susceptible to a NULL pointer dereference issue via RPC-interface. The	N/A	O-MIC-WIND-030523/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue was fixed with Avast and AVG Antivirus version 22.11 **CVE ID : CVE-2023-1587**		
Product: windows_10					
Affected Version(s): -					
Missing Authentication for Critical Function	18-Apr-2023	9.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface. **CVE ID : CVE-2023-29411**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/943
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	9.8	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=S	O-MIC-WIND-030523/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution when manipulating internal methods through Java RMI interface. **CVE ID : CVE-2023-29412**	EVD-2023-101-04.pdf	
Missing Authentication for Critical Function	18-Apr-2023	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service. **CVE ID : CVE-2023-29413**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/945
Product: windows_11					
Affected Version(s): -					
Missing Authentication for	18-Apr-2023	9.8	A CWE-306: Missing Authentication for	https://download.schneider-	O-MIC-WIND-030523/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface. **CVE ID : CVE-2023-29411**	electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	9.8	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29412		
Missing Authentication for Critical Function	18-Apr-2023	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service. **CVE ID : CVE-2023-29413**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/948
Product: windows_server_2016					
Affected Version(s): -					
Missing Authentication for Critical Function	18-Apr-2023	9.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29411		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	9.8	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface. **CVE ID : CVE-2023-29412**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/950
Missing Authentication for Critical Function	18-Apr-2023	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_	O-MIC-WIND-030523/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the Schneider UPS Monitor service. **CVE ID : CVE-2023-29413**	File_Name=SEVD-2023-101-04.pdf	
Product: windows_server_2019					
Affected Version(s): -					
Missing Authentication for Critical Function	18-Apr-2023	9.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface. **CVE ID : CVE-2023-29411**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/952
Improper Neutralization of Special	18-Apr-2023	9.8		https://download.schneider-electric.com/	O-MIC-WIND-030523/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface. **CVE ID : CVE-2023-29412**	files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	
Missing Authentication for Critical Function	18-Apr-2023	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29413		
Product: windows_server_2022					
Affected Version(s): -					
Missing Authentication for Critical Function	18-Apr-2023	9.8	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow changes to administrative credentials, leading to potential remote code execution without requiring prior authentication on the Java RMI interface. **CVE ID : CVE-2023-29411**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/955
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Apr-2023	9.8	A CWE-78: Improper Handling of Case Sensitivity vulnerability exists that could cause remote code execution when manipulating internal methods through Java RMI interface.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29412		
Missing Authentication for Critical Function	18-Apr-2023	7.5	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause Denial-of-Service when accessed by an unauthenticated user on the Schneider UPS Monitor service. **CVE ID : CVE-2023-29413**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-04&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-04.pdf	O-MIC-WIND-030523/957
Vendor: Nvidia					
Product: bmc					
Affected Version(s): * Up to (excluding) 1.08.00					
Out-of-bounds Write	22-Apr-2023	6.7	NVIDIA DGX-2 contains a vulnerability in OFBD where a user with high privileges and a pre-conditioned heap can cause an access	https://nvidia.custhelp.com/app/answers/detail/a_id/5449	O-NVI-BMC-030523/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond a buffers end, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. **CVE ID : CVE-2023-0200**		
Out-of-bounds Write	22-Apr-2023	6.7	NVIDIA DGX-2 SBIOS contains a vulnerability in Bds, where a user with high privileges can cause a write beyond the bounds of an indexable resource, which may lead to code execution, denial of service, compromised integrity, and information disclosure. **CVE ID : CVE-2023-0201**	https://nvidia.custhelp.com/app/answers/detail/a_id/5449	O-NVI-BMC-030523/959
Affected Version(s): * Up to (excluding) 3.39.30					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Apr-2023	8.8	NVIDIA DGX-1 BMC contains a vulnerability in the SPX REST API, where an attacker with the appropriate level of authorization can inject arbitrary shell commands, which may lead to code execution, denial of service, information disclosure, and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	O-NVI-BMC-030523/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25507		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Apr-2023	7.8	NVIDIA DGX-1 BMC contains a vulnerability in the IPMI handler of the AMI MegaRAC BMC , where an attacker with the appropriate level of authorization can cause a buffer overflow, which may lead to denial of service, information disclosure, or arbitrary code execution. **CVE ID : CVE-2023-25505**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	O-NVI-BMC-030523/961
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Apr-2023	7.8	NVIDIA DGX-1 BMC contains a vulnerability in the IPMI handler, where an attacker with the appropriate level of authorization can upload and download arbitrary files under certain circumstances, which may lead to denial of service, escalation of privileges, information disclosure, and data tampering. **CVE ID : CVE-2023-25508**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	O-NVI-BMC-030523/962
Product: sbios					
Affected Version(s): * Up to (excluding) 0.33					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	22-Apr-2023	4.4	NVIDIA DGX-2 SBIOS contains a vulnerability where an attacker may modify the ServerSetup NVRAM variable at runtime by executing privileged code. A successful exploit of this vulnerability may lead to denial of service. **CVE ID : CVE-2023-0207**	https://nvidia.custhelp.com/app/answers/detail/a_id/5449	O-NVI-SBIO-030523/963
Affected Version(s): * Up to (excluding) 52w_3a13					
Out-of-bounds Write	22-Apr-2023	8.2	NVIDIA DGX-1 contains a vulnerability in Ofbd in AMI SBIOS, where a preconditioned heap can allow a user with elevated privileges to cause an access beyond the end of a buffer, which may lead to code execution, escalation of privileges, denial of service and information disclosure. The scope of the impact of this vulnerability can extend to other components. **CVE ID : CVE-2023-25506**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	O-NVI-SBIO-030523/964
Improper Authentication	22-Apr-2023	7.8	NVIDIA DGX-1 SBIOS contains a vulnerability in the Uncore PEI module, where authentication	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	O-NVI-SBIO-030523/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the code executed by SSA is missing, which may lead to arbitrary code execution, denial of service, escalation of privileges assisted by a firmware implant, information disclosure assisted by a firmware implant, data tampering, and SecureBoot bypass. **CVE ID : CVE-2023-0209**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Apr-2023	7.8	NVIDIA DGX-1 SBIOS contains a vulnerability in Bds, which may lead to code execution, denial of service, and escalation of privileges. **CVE ID : CVE-2023-25509**	https://nvidia.custhelp.com/app/answers/detail/a_id/5458	O-NVI-SBIO-030523/966
Vendor: Oracle					
Product: solaris					
Affected Version(s): 10					
N/A	18-Apr-2023	7.8	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Core). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21948**		
N/A	18-Apr-2023	7.7	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21985**		
N/A	18-Apr-2023	7	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21896**	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Apr-2023	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22003**	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/970
Affected Version(s): 11					
N/A	18-Apr-2023	7.7	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10 and 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21985**		
N/A	18-Apr-2023	7	Vulnerability in the Oracle Solaris product of Oracle Systems (component: NSSwitch). Supported versions that are affected are 10 and 11. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-21896**		
N/A	18-Apr-2023	6.5	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Libraries). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21984**		
N/A	18-Apr-2023	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22003		
N/A	18-Apr-2023	1.8	Vulnerability in the Oracle Solaris product of Oracle Systems (component: IPS repository daemon). The supported version that is affected is 11. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21928**	https://www.oracle.com/security-alerts/cpuapr2023.html	O-ORA-SOLA-030523/975
Vendor: Phoenixcontact					
Product: infobox_firmware					
Affected Version(s): From (including) 01.00.00.00 Up to (including) 02.02.00.00					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**	N/A	O-PHO-INFO-030523/976
Product: smartrtu_axc_ig_firmware					
Affected Version(s): From (including) 01.00.00.00 Up to (including) 01.02.00.01					
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**	N/A	O-PHO-SMAR-030523/977
Product: smartrtu_axc_sg_firmware					
Affected Version(s): From (including) 01.00.00.00 Up to (including) 01.08.00.02					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Apr-2023	8.8	In Phoenix Contacts ENERGY AXC PU Web service an authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service. This may lead to full control of the service. **CVE ID : CVE-2023-1109**	N/A	O-PHO-SMAR-030523/978
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Out-of-bounds Write	20-Apr-2023	6.7	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution. **CVE ID : CVE-2023-2194**	https://bugzilla.redhat.com/show_bug.cgi?id=2188396, https://github.com/torvalds/linux/commit/92fbb6d1296f	O-RED-ENTE-030523/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	19-Apr-2023	5.5	A NULL pointer dereference flaw was found in the UNIX protocol in net/unix/diag.c In unix_diag_get_exact in the Linux Kernel. The newly allocated skb does not have sk, leading to a NULL pointer. This flaw allows a local user to crash or potentially cause a denial of service. **CVE ID : CVE-2023-28327**	https://bugzilla.redhat.com/show_bug.cgi?id=2177382	O-RED-ENTE-030523/980
NULL Pointer Dereference	19-Apr-2023	5.5	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Linux Kernel. The message from user space is not checked properly before transferring into the device. This flaw allows a local user to crash the system or potentially cause a denial of service. **CVE ID : CVE-2023-28328**	https://bugzilla.redhat.com/show_bug.cgi?id=2177389	O-RED-ENTE-030523/981
Affected Version(s): 9.0					
Out-of-bounds Write	20-Apr-2023	6.7	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data-	https://bugzilla.redhat.com/show_bug.cgi?id=2188396, https://githu	O-RED-ENTE-030523/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			>block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw could allow a local privileged user to crash the system or potentially achieve code execution. **CVE ID : CVE-2023-2194**	b.com/torvalds/linux/commit/92fbb6d1296f	
NULL Pointer Dereference	19-Apr-2023	5.5	A NULL pointer dereference flaw was found in the UNIX protocol in net/unix/diag.c In unix_diag_get_exact in the Linux Kernel. The newly allocated skb does not have sk, leading to a NULL pointer. This flaw allows a local user to crash or potentially cause a denial of service. **CVE ID : CVE-2023-28327**	https://bugzilla.redhat.com/show_bug.cgi?id=2177382	O-RED-ENTE-030523/983
Vendor: Schneider-electric					
Product: 140cpu65_firmware					
Affected Version(s): *					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional	N/A	O-SCH-140C-030523/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**		
Product: bmeh58s_firmware					
Affected Version(s): *					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**	N/A	O-SCH-BMEH-030523/985
Improper Check for Unusual or	19-Apr-2023	6.5		N/A	O-SCH-BMEH-030523/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**		
Product: bmep58s_firmware					
Affected Version(s): *					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.	N/A	O-SCH-BMEP-030523/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25619		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	O-SCH-BMEP-030523/988
Product: conext_gateway_firmware					
Affected Version(s): * Up to (excluding) 1.16					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=S	O-SCH-CONE-030523/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	EVD-2023-101-02.pdf	
Affected Version(s): 1.16					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	O-SCH-CONE-030523/990
Product: insightfacility_firmware					
Affected Version(s): * Up to (excluding) 1.16					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	O-SCH-INSI-030523/991
Affected Version(s): 1.16					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute.	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	O-SCH-INSI-030523/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29410		
Product: insighthome_firmware					
Affected Version(s): * Up to (excluding) 1.16					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	O-SCH-INSI-030523/993
Affected Version(s): 1.16					
Improper Input Validation	18-Apr-2023	8.8	A CWE-20: Improper Input Validation vulnerability exists	https://download.schneider-electric.com/files?p_Doc_	O-SCH-INSI-030523/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that could allow an authenticated attacker to gain the same privilege as the application on the server when a malicious payload is provided over HTTP for the server to execute. **CVE ID : CVE-2023-29410**	Ref=SEVD-2023-101-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-101-02.pdf	
Product: merten_instabus_tastermodul_1fach_system_m_firmware					
Affected Version(s): 1.0					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/995
Product: merten_instabus_tastermodul_2fach_system_m_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/996
Product: merten_jalousie-\/schaltaktor_reg-k\/8x\/16x\/10_m._hb_firmware					
Affected Version(s): 1.0					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/997
Product: merten_knx_argus_180\/2\,20m_up_system_firmware					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/998
Product: merten_knx_schaltakt.2x6a_up_m.2_eing._firmware					
Affected Version(s): 0.1					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/999
Product: merten_knx_uni-dimmaktor_ll_reg-k\/2x230\/300_w_firmware					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/1000
Affected Version(s): 1.1					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/1001
Product: merten_tasterschnittstelle_4fach_plus_firmware					
Affected Version(s): 1.0					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication	https://download.schneider-	O-SCH-MERT-030523/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	
Affected Version(s): 1.2					
Improper Authentication	18-Apr-2023	8.8	A CWE-287: Improper Authentication vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation. **CVE ID : CVE-2023-25556**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-03.pdf	O-SCH-MERT-030523/1003
Product: modicon_m340_firmware					
Affected Version(s): * Up to (excluding) 3.51					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions	N/A	O-SCH-MODI-030523/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	O-SCH-MODI-030523/1005
Product: modicon_m580_firmware					
Affected Version(s): * Up to (excluding) 4.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**	N/A	O-SCH-MODI-030523/1006
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.	N/A	O-SCH-MODI-030523/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25620		
Product: modicon_mc80_firmware					
Affected Version(s): *					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**	N/A	O-SCH-MODI-030523/1008
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.	N/A	O-SCH-MODI-030523/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25620		
Product: modicon_momentum_unity_m1e_processor_firmware					
Affected Version(s): *					
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	7.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**	N/A	O-SCH-MODI-030523/1010
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the	N/A	O-SCH-MODI-030523/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller by an authenticated user. **CVE ID : CVE-2023-25620**		
Product: powerlogic_hdpm6000_firmware					
Affected Version(s): * Up to (including) 0.58.6					
Improper Validation of Array Index	18-Apr-2023	9.8	A CWE-129: Improper validation of an array index vulnerability exists where a specially crafted Ethernet request could result in denial of service or remote code execution. **CVE ID : CVE-2023-28004**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-073-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-073-02.pdf	O-SCH-POWE-030523/1012
Product: tsxp57_firmware					
Affected Version(s): *					
Improper Check for	19-Apr-2023	7.5		N/A	O-SCH-TSXP-030523/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol. **CVE ID : CVE-2023-25619**		
Improper Check for Unusual or Exceptional Conditions	19-Apr-2023	6.5	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user. **CVE ID : CVE-2023-25620**	N/A	O-SCH-TSXP-030523/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Tenda					
Product: ac15_firmware					
Affected Version(s): 15.03.05.19					
Out-of-bounds Write	24-Apr-2023	9.8	Tenda AC15 V15.03.05.19 is vulnerable to Buffer Overflow. **CVE ID : CVE-2023-30369**	N/A	O-TEN-AC15-030523/1015
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function GetValue contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30370**	N/A	O-TEN-AC15-030523/1016
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "sub_ED14" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30371**	N/A	O-TEN-AC15-030523/1017
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, The function "xkjs_ver32" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30372**	N/A	O-TEN-AC15-030523/1018
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "xian_pppoe_user" contains a stack-based buffer overflow vulnerability.	N/A	O-TEN-AC15-030523/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30373		
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "getIfIp" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30375**	N/A	O-TEN-AC15-030523/1020
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "henan_pppoe_user" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30376**	N/A	O-TEN-AC15-030523/1021
Out-of-bounds Write	24-Apr-2023	9.8	In Tenda AC15 V15.03.05.19, the function "sub_8EE8" contains a stack-based buffer overflow vulnerability. **CVE ID : CVE-2023-30378**	N/A	O-TEN-AC15-030523/1022
Product: ac5_firmware					
Affected Version(s): 15.03.06.28					
Out-of-bounds Write	24-Apr-2023	9.8	Tenda AC5 V15.03.06.28 is vulnerable to Buffer Overflow via the initWebs function. **CVE ID : CVE-2023-30368**	N/A	O-TEN-AC5_-030523/1023
Vendor: tribe29					
Product: checkmk_appliance_firmware					
Affected Version(s): * Up to (excluding) 1.6.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Apr-2023	6.1	Reflective Cross-Site-Scripting in Webconf in Tribe29 Checkmk Appliance before 1.6.4. **CVE ID : CVE-2023-22309**	https://checkmk.com/werk/9523	O-TRI-CHEC-030523/1024
Exposure of Resource to Wrong Sphere	18-Apr-2023	5.5	Sensitive data exposure in Webconf in Tribe29 Checkmk Appliance before 1.6.4 allows local attacker to retrieve passwords via reading log files. **CVE ID : CVE-2023-22307**	https://checkmk.com/werk/9522	O-TRI-CHEC-030523/1025