

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للتُغرات المسجلة national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology the National Institute of Standards and Technology (NIST) من قبل (NIST) National Vulnerability Database (NVD) for the week from 8th of 14 للأسبوع من 8 اكتوبر إلى National Vulnerability Database (NVD) October to 14th of October. Vulnerabilities are scored using the Common اكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار (CVSS) Standard as per the حيث يتم تصنيف الثغرات بناء على Vulnerability Scoring System (CVSS) following severity:

Critical: CVSS base score of 9.0-10.0 High: CVSS base score of 7.0-8.9 Medium: CVSS base score 4.0-6.9 Low: CVSS base score 0.0-3.9

التالي:

عالى جدًا: النتيجة الأساسية لـ10.0-CVSS 9.0

عالى: النتيجة الأساسية لـCVSS 7.0-8.9

متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0

منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

Vendor - Product **Publish Date** Score Severity CVE ID & Source Description A directory traversal vulnerability exists in the BIG-IP Configuration Utility that may allow an authenticated attacker to execute commands on the BIG-IP system. For BIG-IP system running in Appliance mode, a successful exploit can allow the attacker to cross a security boundary. f5 - multiple Note: Software versions which have reached End of Technical CVE-2023-41373 products Support (EoTS) are not evaluated. 2023-10-10 9.9 Critical HP LIFE Android Mobile application is potentially vulnerable to CVE-2023-5365 hp - life escalation of privilege and/or information disclosure. 2023-10-09 9.8 Critical A vulnerability has been identified in Simcenter Amesim (All versions < V2021.1). The affected application contains a SOAP endpoint that could allow an unauthenticated remote attacker to perform DLL injection and execute arbitrary code in the context of siemens -CVE-2023-43625 the affected application process. 2023-10-10 9.8 Critical simcenter_amesim A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.0.0 and 6.7.0 through 6.7.5 and 6.6.0 through 6.6.3 and 6.5.0 fortinet - multiple through 6.5.1 and 6.4.0 through 6.4.2 allows attacker to execute CVE-2023-34992 products unauthorized code or commands via crafted API requests. 2023-10-10 9.8 Critical A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to fortinet - multiple execute unauthorized code or commands via specifically crafted http get request parameters. CVE-2023-34993 products 2023-10-10 9.8 Critical A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to fortinet - multiple execute unauthorized code or commands via specifically crafted CVE-2023-36547 2023-10-10 9.8 Critical products http get request parameters. A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to fortinet - multiple execute unauthorized code or commands via specifically crafted CVE-2023-36548 http get request parameters. 2023-10-10 9.8 Critical products A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted fortinet - multiple CVE-2023-36549 9.8 Critical products 2023-10-10 http get request parameters. A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to fortinet - multiple execute unauthorized code or commands via specifically crafted CVE-2023-36550 http get request parameters. Critical products 2023-10-10 9.8 microsoft - multiple CVE-2023-35349 products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 9.8 Critical

مـتـاح

	microsoft -	Azure HDInsight Apache Oozie Workflow Scheduler Elevation of			
CVE-2023-36419	azure_hdinsights microsoft - multiple	Privilege Vulnerability	2023-10-10	9.8	Critical
CVE-2023-36434	products	Windows IIS Server Elevation of Privilege Vulnerability	2023-10-10	9.8	Critical
		API permission management vulnerability in the Fwk-Display			
CVE-2023-44106	huawei - multiple products	module.Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-10-11	9.8	Critical
<u> </u>	products	Vulnerability of permissions not being strictly verified in the	2020 10 11	3.0	Citical
CVE 2022 444.0F	huawei - multiple	window management module. Successful exploitation of this	2022 40 44	0.0	Ciliant
CVE-2023-44105	products	vulnerability may cause features to perform abnormally. Vulnerability of access permissions not being strictly verified in the	2023-10-11	9.8	Critical
	huawei - multiple	APPWidget module.Successful exploitation of this vulnerability			
CVE-2023-44116	products	may cause some apps to run without being authorized.	2023-10-11	9.8	Critical
		In TBD of TBD, there is a possible stack buffer overflow due to a missing bounds check. This could lead to remote code execution			
		with no additional execution privileges needed. User interaction is			
CVE-2023-35646	google - android	not needed for exploitation. In ProtocolEmbmsGlobalCellIdAdapter::Init() of	2023-10-11	9.8	Critical
		protocolembmsadapter.cpp, there is a possible out of bounds read			
		due to a missing bounds check. This could lead to remote			
CVE-2023-35647	google - android	information disclosure with baseband firmware compromise required. User interaction is not needed for exploitation.	2023-10-11	9.8	Critical
CVL 2023 330+7	googie unaroid	In ProtocolMiscLceIndAdapter::GetConfLevel() of	2023 10 11	3.0	Critical
		protocolmiscadapter.cpp, there is a possible out of bounds read			
		due to a missing bounds check. This could lead to remote information disclosure with baseband firmware compromise			
CVE-2023-35648	google - android	required. User interaction is not needed for exploitation.	2023-10-11	9.8	Critical
		there is a possible out of bounds write due to buffer overflow. This			
CVE-2023-35662	google - android	could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-11	9.8	Critical
	0.00	An improper access control vulnerability [CWE-284] in			
		FortiManager management interface 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions			
		may allow a remote and authenticated attacker with at least			
	fortinet - multiple	"device management" permission on his profile and belonging to a			
CVE-2023-41679	products	specific ADOM to add and delete CLI script on other ADOMs Authorization Bypass Through User-Controlled Key vulnerability in	2023-10-10	9.6	Critical
		Apache ZooKeeper. If SASL Quorum Peer authentication is enabled			
		in ZooKeeper (quorum.auth.enableSasl=true), the authorization is			
		done by verifying that the instance part in SASL authentication ID is listed in zoo.cfg server list. The instance part in SASL auth ID is			
		optional and if it's missing, like 'eve@EXAMPLE.COM', the			
		authorization check will be skipped. As a result an arbitrary			
		endpoint could join the cluster and begin propagating counterfeit changes to the leader, essentially giving it complete read-write			
		access to the data tree. Quorum Peer authentication is not			
		enabled by default.			
		Users are recommended to upgrade to version 3.9.1, 3.8.3, 3.7.2,			
		which fixes the issue.			
		Alternately encurs the encomble election/guerum communication			
		Alternately ensure the ensemble election/quorum communication is protected by a firewall as this will mitigate the issue.			
CVE-2023-44981	apache - multiple products	See the documentation for more details on correct cluster administration.	2023-10-11	9.1	Critical
OVE 2023-44301	products	Vulnerability of defects introduced in the design process in the	2023 10-11	J.1	Citical
01/5 2002 11:55	huawei -	screen projection module. Successful exploitation of this	2022 12 11		6
CVE-2023-44107	harmonyos	vulnerability may affect service availability and integrity. Vulnerability of undefined permissions in the MeeTime	2023-10-11	9.1	Critical
	huawei - multiple	module.Successful exploitation of this vulnerability will affect			
CVE-2023-44118	products	availability and confidentiality.	2023-10-11	9.1	Critical
CVE-2023-32723	zabbix - multiple products	Request to LDAP is sent before user permissions are checked.	2023-10-12	9.1	Critical
	F 22.3.66	IBM Security Directory Server 6.4.0 is vulnerable to an XML			
		External Entity Injection (XXE) attack when processing XML data. A			
	ibm - multiple	remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID:			
CVE-2022-32755	products	228505.	2023-10-14	9.1	Critical
		A vulnerability has been identified in CP-8031 MASTER MODULE			
		(All versions < CPCI85 V05.11), CP-8050 MASTER MODULE (All versions < CPCI85 V05.11). The web server of affected devices fails			
		to properly sanitize user input for the /sicweb-ajax/tmproot/			
		endpoint.			
CVE-2023-42796	siemens - cp- 8050_firmware	This could allow an authenticated remote attacker to traverse directories on the system and download arbitrary files. By	2023-10-10	8.8	High
CVL-2023-42/30		an ectories on the system and download arbitrary illes. By	7072-10-10	0.0	ııığıı

	T			ı	
		exploring active session IDs, the vulnerability could potentially be leveraged to escalate privileges to the administrator role.			
		A improper neutralization of special elements used in an os			
		command ('os command injection') in Fortinet FortiWLM version			
		8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to			
	fortinet - multiple	execute unauthorized code or commands via specifically crafted			
CVE-2023-34985	products	HTTP get request parameters.	2023-10-10	8.8	High
	'	A improper neutralization of special elements used in an os			
		command ('os command injection') in Fortinet FortiWLM version			
		8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to			
	fortinet - multiple	execute unauthorized code or commands via specifically crafted			
CVE-2023-34986	products	HTTP get request parameters.	2023-10-10	8.8	High
	'	A improper neutralization of special elements used in an os			
		command ('os command injection') in Fortinet FortiWLM version			
		8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to			
	fortinet - multiple	execute unauthorized code or commands via specifically crafted			
CVE-2023-34987	products	HTTP get request parameters.	2023-10-10	8.8	High
	'	A improper neutralization of special elements used in an os			
		command ('os command injection') in Fortinet FortiWLM version			
		8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to			
	fortinet - multiple	execute unauthorized code or commands via specifically crafted			
CVE-2023-34988	products	HTTP get request parameters.	2023-10-10	8.8	High
CVL-2023-34300	products	A improper neutralization of special elements used in an os	2023-10-10	0.0	iligii
		command ('os command injection') in Fortinet FortiWLM version			
	fortingt multiple	8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to			
CVE 2022 24000	fortinet - multiple	execute unauthorized code or commands via specifically crafted	2022 40 40	0.0	مام :الا
CVE-2023-34989	products	HTTP get request parameters.	2023-10-10	8.8	High
		An incorrect authorization vulnerability [CWE-863] in FortiMail			
		webmail version 7.2.0 through 7.2.2, version 7.0.0 through 7.0.5			
	6	and below 6.4.7 allows an authenticated attacker to login on other			
	fortinet - multiple	users accounts from the same web domain via crafted HTTP or			
CVE-2023-36556	products	HTTPs requests.	2023-10-10	8.8	High
		An improper authorization vulnerability in Fortinet FortiOS 7.0.0 -			
	fortinet - multiple	7.0.11 and 7.2.0 - 7.2.4 allows an attacker belonging to the prof-			
CVE-2023-41841	products	admin profile to perform elevated actions.	2023-10-10	8.8	High
	microsoft -				
CVE-2023-36414	azure_identity_sdk	Azure Identity SDK Remote Code Execution Vulnerability	2023-10-10	8.8	High
	microsoft - multiple				
CVE-2023-36415	products	Azure Identity SDK Remote Code Execution Vulnerability	2023-10-10	8.8	High
	microsoft - multiple	Microsoft WDAC OLE DB provider for SQL Server Remote Code			
CVE-2023-36577	products	Execution Vulnerability	2023-10-10	8.8	High
	apache - multiple	An integer overflow in xerces-c++ 3.2.3 in BigFix Platform allows			
CVE-2023-37536	products	remote attackers to cause out-of-bound access via HTTP request.	2023-10-11	8.8	High
		Use after free in Site Isolation in Google Chrome prior to			
		118.0.5993.70 allowed a remote attacker to potentially exploit			
		heap corruption via a crafted HTML page. (Chromium security			
CVE-2023-5218	google - chrome	severity: Critical)	2023-10-11	8.8	High
	0 0	Heap buffer overflow in PDF in Google Chrome prior to			
		118.0.5993.70 allowed a remote attacker who convinced a user to			
		engage in specific user interactions to potentially exploit heap			
		corruption via a crafted PDF file. (Chromium security severity:			
CVE-2023-5474	google - chrome	Medium)	2023-10-11	8.8	High
CVL 2023 3474	googie emonie	Use after free in Blink History in Google Chrome prior to	2023 10 11	0.0	111611
		, , , , , , , , , , , , , , , , , , , ,			
		118.0.5993.70 allowed a remote attacker to potentially exploit			
CVE_2022 E476	google chrome	heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-10-11	8.8	ام،نا
CVE-2023-5476	google - chrome	·	∠U∠3-1U-11	0.8	High
	and halo on the t	Memory pointer is in a property of the Ducktape object. This leads			
C) /E 2022 22== :	zabbix - multiple	to multiple vulnerabilities related to direct memory access and	2022 42 42		
CVE-2023-32724	products	manipulation.	2023-10-12	8.8	High
		SnapCenter versions 3.x and 4.x prior to 4.9 are susceptible to a			
		vulnerability which may allow an authenticated unprivileged user			
	netapp -	to gain		_	
CVE-2023-27313	snapcenter	access as an admin user.	2023-10-12	8.8	High
		An Unchecked Return Value vulnerability in the user interfaces to			
		the Juniper Networks Junos OS and Junos OS Evolved, the CLI, the			
		XML API, the XML Management Protocol, the NETCONF			
		Management Protocol, the gNMI interfaces, and the J-Web User			
		Interfaces causes unintended effects such as demotion or			
		elevation of privileges associated with an operators actions to			
		occur.			
		Multiple scenarios may occur; for example: privilege escalation			
		over the device or another account, access to files that should not			
		otherwise be accessible, files not being accessible where they			
		should be accessible, code expected to run as non-root may run as			
		root, and so forth.			
	juniper - multiple				
CVE-2023-44182	products	This issue affects:	2023-10-13	8.8	High
	1	I .			

		Juniper Networks Junos OS			
		* All versions prior to 20.4R3-S7; * 21.1 versions prior to 21.1R3-S5; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R2-S2, 22.2R3; * 22.3 versions prior to 22.3R1-S2, 22.3R2.			
		Juniper Networks Junos OS Evolved			
		* All versions prior to 21.4R3-S3-EVO; * 22.1-EVO version 22.1R1-EVO and later versions prior to 22.2R2-S2-EVO, 22.2R3-EVO; * 22.3-EVO versions prior to 22.3R1-S2-EVO, 22.3R2-EVO.			
CVE-2023-38218	adobe - multiple products	Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by an improper input validation vulnerability. An authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation.	2023-10-13	8.8	High
		A SQL injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network.			
CVE-2023-34975	qnap - video_station	We have already fixed the vulnerability in the following version: Video Station 5.7.0 (2023/07/27) and later A SQL injection vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network.	2023-10-13	8.8	High
<u>CVE-2023-34976</u>	qnap - video_station	We have already fixed the vulnerability in the following version: Video Station 5.7.0 (2023/07/27) and later	2023-10-13	8.8	High
CVE-2023-43746	f5 - multiple products	When running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing BIG-IP external monitor on a BIG-IP system. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	2023-10-10	8.7	High
CVE-2023-38219	adobe - multiple products	executed in a victim's browser when they browse to the page containing the vulnerable field. Payload is stored in an admin area, resulting in high confidentiality and integrity impact.	2023-10-13	8.7	High
CVE-2023-36569	microsoft - multiple products	Microsoft Office Elevation of Privilege Vulnerability	2023-10-10	8.4	High
		An authenticated user's session cookie may remain valid for a limited time after logging out from the BIG-IP Configuration utility on a multi-blade VIPRION platform. Note: Software versions which have reached End of Technical			
	f5 - multiple	Support (EoTS) are not evaluated.			
CVE-2023-40537	products microsoft - multiple		2023-10-10	8.1	High
CVE-2023-38166	products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High

microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1 microsoft - multiple products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1	High High High
CVE-2023-41768productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1CVE-2023-41769productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1microsoft - multiple CVE-2023-41770productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1microsoft - multiple CVE-2023-41771productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1microsoft - multiple CVE-2023-41773microsoft - multiple productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1	High
CVE-2023-41769productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1CVE-2023-41770productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1CVE-2023-41771productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1microsoft - multiple CVE-2023-41773microsoft - multiple productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1	
CVE-2023-41770productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1CVE-2023-41771productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1CVE-2023-41773microsoft - multiple productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1	High
CVE-2023-41771productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1microsoft - multiple CVE-2023-41773productsLayer 2 Tunneling Protocol Remote Code Execution Vulnerability2023-10-108.1	
CVE-2023-41773 products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1	High
	High
microsoft - multiple CVE-2023-41774 products Layer 2 Tunneling Protocol Remote Code Execution Vulnerability 2023-10-10 8.1	High
A insufficient session expiration in Fortinet FortiEDR version 5.0.0	Iligii
through 5.0.1 allows attacker to execute unauthorized code or commands via api request 2023-10-13 8.1	High
microsoft - multiple CVE-2023-36697 products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 8	High
microsoft - multiple CVE-2023-36778 products Microsoft Exchange Server Remote Code Execution Vulnerability 2023-10-10 8	High
In phasechecksercer, there is a possible missing permission check. google - multiple This could lead to local escalation of privilege with no additional	
CVE-2023-40634 products execution privileges needed 2023-10-08 7.8	High
In linkturbo, there is a possible missing permission check. This could lead to local escalation of privilege with no additional	
CVE-2023-40635google - androidexecution privileges needed2023-10-087.8A potential vulnerability in a driver used during manufacturing	High
process on some consumer Lenovo Notebook devices that was	
lenovo - mistakenly not deactivated may allow an attacker with elevated ideapad_creator_5- privileges to modify secure boot setting by modifying an NVRAM	
<u>CVE-2022-3431</u> 16ach6_firmware variable. 2023-10-09 7.8	High
A vulnerability has been identified in SINEC NMS (All versions < V2.0). The affected application assigns improper access rights to	
specific folders containing executable files and libraries.	
siemens - This could allow an authenticated local attacker to inject arbitrary	
CVE-2022-30527sinec_nmscode and escalate privileges.2023-10-107.8	High
A vulnerability has been identified in Xpedition Layout Browser (All siemens - versions < VX.2.14). Affected application contains a stack overflow	
xpedition_layout_b vulnerability when parsing a PCB file. An attacker can leverage this	112.16
CVE-2023-30900rowservulnerability to execute code in the context of the current process.2023-10-107.8A vulnerability has been identified in CP-8031 MASTER MODULE	High
(All versions < CPCI85 V05.11 (only with activated debug support)), CP-8050 MASTER MODULE (All versions < CPCI85 V05.11 (only	
with activated debug support)). The affected devices contain a	
hard-coded ID in the SSH `authorized_keys` configuration file. An attacker with knowledge of the corresponding private key could	
siemens - cp- login to the device via SSH. Only devices with activated debug	
CVE-2023-363808050_firmwaresupport are affected.2023-10-107.8A vulnerability has been identified in Tecnomatix Plant Simulation	High
V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation	
V2302 (All versions < V2302.0003). The affected application contains an out of bounds write past the end of an allocated buffer	
siemens - multiple while parsing a specially crafted SPP file. This could allow an	High
CVE-2023-44081productsattacker to execute code in the context of the current process.2023-10-107.8A vulnerability has been identified in Tecnomatix Plant Simulation	High
V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected application	
contains an out of bounds write past the end of an allocated buffer	
siemens - multiple while parsing a specially crafted SPP file. This could allow an CVE-2023-44082 products attacker to execute code in the context of the current process. 2023-10-10 7.8	High
A vulnerability has been identified in Tecnomatix Plant Simulation	111811
V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected application	
contains an out of bounds write past the end of an allocated buffer	
siemens - multiple while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process. 2023-10-10 7.8	High
A vulnerability has been identified in Tecnomatix Plant Simulation	_
V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications	
contain an out of bounds read past the end of an allocated siemens - multiple structure while parsing specially crafted SPP files. This could allow	
CVE-2023-44084 products an attacker to execute code in the context of the current process. 2023-10-10 7.8	High
A vulnerability has been identified in Tecnomatix Plant Simulation siemens - multiple V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation	
<u>CVE-2023-44085</u> products V2302 (All versions < V2302.0003). The affected applications 2023-10-10 7.8	High

CVE-2023-44086	iemens - multiple products	contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain an out of bounds read past the end of an allocated			
<u>CVE-2023-44086</u>	•	an attacker to execute code in the context of the current process. A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications			
<u>CVE-2023-44086</u>	•	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications			
<u>CVE-2023-44086</u>	•	V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications			
<u>CVE-2023-44086</u>	•	V2302 (All versions < V2302.0003). The affected applications			
<u>CVE-2023-44086</u>	•	,			
<u>CVE-2023-44086</u>	•	CONTAIN AN OUT OF DOUNDS LEAD DAST THE END OF AN ANOCATED			
<u>CVE-2023-44086</u>	•	structure while parsing specially crafted SPP files. This could allow			
si	products	an attacker to execute code in the context of the current process.	2023-10-10	7.8	High
			2025-10-10	7.6	півіі
		A vulnerability has been identified in Tecnomatix Plant Simulation			
		V2201 (All versions < V2201.0009), Technomatix Plant Simulation			
		V2302 (All versions < V2302.0003). The affected applications			
	iomons multiplo	contain an out of bounds read past the end of an allocated			
CVE-2023-44087	iemens - multiple	structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	2023-10-10	7.8	Hiah
	products	A vulnerability has been identified in Tecnomatix Plant Simulation	2023-10-10	7.0	High
		V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation			
		, , , , , , , , , , , , , , , , , , , ,			
		V2302 (All versions < V2302.0003). The affected applications			
a:	وامتطابيهم وموسون	contain a type confusion vulnerability while parsing specially			
	iemens - multiple	crafted IGS files. This could allow an attacker to execute code in	2023-10-10	7.0	Hiah
CVE-2023-45204	products	the context of the current process. (ZDI-CAN-21268)	2023-10-10	7.8	High
		A vulnerability has been identified in SICAM PAS/PQS (All versions			
		>= V8.00 < V8.20). The affected application is installed with			
		specific files and folders with insecure permissions. This could			
0) (5, 2022, 45225	siemens -	allow an authenticated local attacker to inject arbitrary code and	2022 40 40	7.0	
CVE-2023-45205	sicam_pas√pqs	escalate privileges to `NT AUTHORITY/SYSTEM`.	2023-10-10	7.8	High
		A vulnerability has been identified in Parasolid V35.0 (All versions			
		< V35.0.262), Parasolid V35.1 (All versions < V35.1.250), Parasolid			
		V36.0 (All versions < V36.0.169), Tecnomatix Plant Simulation			
		V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation			
		V2302 (All versions < V2302.0003). The affected applications			
		contain a stack overflow vulnerability while parsing specially			
	iemens - multiple	crafted IGS files. This could allow an attacker to execute code in			
CVE-2023-45601	products	the context of the current process. (ZDI-CAN-21290)	2023-10-10	7.8	High
		The BIG-IP Edge Client Installer on macOS does not follow best			
		practices for elevating privileges during the installation			
		process. This vulnerability is due to an incomplete fix for CVE-			
	f5 - multiple	2023-38418. Note: Software versions which have reached End of			
CVE-2023-43611	products	Technical Support (EoTS) are not evaluated	2023-10-10	7.8	High
		An insufficient verification of data vulnerability exists in BIG-IP			
		Edge Client Installer on macOS that may allow an attacker			
		elevation of privileges during the installation process.			
		Note: Software versions which have reached End of Technical			
		Support (EoTS) are not evaluated.			
	f5 - multiple				
CVE-2023-5450	products		2023-10-10	7.8	High
		A improper neutralization of special elements used in an os			
l		command ('os command injection') in Fortinet Fortilsolator version			
		1.0.0, Fortilsolator version 1.1.0, Fortilsolator version 1.2.0			
		through 1.2.2. Fortilsolator version 2.0.0 through 2.0.1.			
		through 1.2.2, Fortilsolator version 2.0.0 through 2.0.1, Fortilsolator version 2.1.0 through 2.1.2 Fortilsolator version			
		Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version			
6.	ortinot multiple	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to			
	fortinet - multiple	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via	2022 40 40	7.0	l II ala
	fortinet - multiple products	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters.	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.2.2, 7.0.0 through 6.4.11, 6.2 all	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.2.2, 7.0.0 through 6.4.11, 6.2 all	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3,	2023-10-10	7.8	High
	•	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ	2023-10-10	7.8	High
CVE-2022-22298	products	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on	2023-10-10	7.8	High
CVE-2022-22298	products .	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp			
CVE-2022-22298	products	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function.	2023-10-10	7.8	High
CVE-2022-22298	products .	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os			
CVE-2022-22298	products .	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in			
CVE-2022-22298	products .	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through			
CVE-2022-22298	products .	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.8, version 6.4.0 through 6.4.12 and			
CVE-2022-22298 for CVE-2023-25607	products fortinet - multiple products	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.8, version 6.4.0 through 6.4.12 and version 6.2.0 through 6.2.11 may allow a local attacker with low			
CVE-2022-22298 CVE-2023-25607	products Fortinet - multiple products Fortinet - multiple	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.8, version 6.4.0 through 6.4.12 and version 6.2.0 through 6.2.11 may allow a local attacker with low privileges to execute unauthorized code via specifically crafted	2023-10-10	7.8	High
CVE-2023-25607 fc	products fortinet - multiple products	Fortilsolator version 2.1.0 through 2.1.2, Fortilsolator version 2.2.0, Fortilsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters. An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function. An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.8, version 6.4.0 through 6.4.12 and version 6.2.0 through 6.2.11 may allow a local attacker with low			

	T			Γ	T
	microsoft - azure_rtos_guix_st				
CVE-2023-36418	udio	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	Microsoft ODBC Driver for SQL Server Remote Code Execution			
CVE-2023-36420	products	Vulnerability	2023-10-10	7.8	High
CVE 2022 26426	microsoft - multiple	Minds a MCHTAN Platform Barrets Code For the William Hills	2022 40 40	7.0	112.1
CVE-2023-36436	products microsoft - multiple	Windows MSHTML Platform Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36557	products	PrintHTML API Remote Code Execution Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	,			
CVE-2023-36594	products	Windows Graphics Component Elevation of Privilege Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	Microsoft WDAC ODBC Driver Remote Code Execution			
CVE-2023-36598	products microsoft - multiple	Vulnerability Windows Named Bine Filesystem Floration of Brivilles	2023-10-10	7.8	High
CVE-2023-36605	products	Windows Named Pipe Filesystem Elevation of Privilege Vulnerability	2023-10-10	7.8	High
<u>CVL 2023 30003</u>	microsoft - multiple	Microsoft Resilient File System (ReFS) Elevation of Privilege	2023 10 10	7.0	111811
CVE-2023-36701	products	Vulnerability	2023-10-10	7.8	High
	microsoft - multiple				
CVE-2023-36702	products	Microsoft DirectMusic Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36704	microsoft - multiple products	Windows Setup Files Cleanup Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVL-2023-30704	microsoft - multiple	Windows Media Foundation Core Remote Code Execution	2023-10-10	7.0	Iligii
CVE-2023-36710	products	Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	Windows Runtime C++ Template Library Elevation of Privilege			
CVE-2023-36711	products	Vulnerability	2023-10-10	7.8	High
CVF_2022 26712	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-10-10	7.8	∐iah
CVE-2023-36712	microsoft - multiple	Microsoft Virtual Trusted Platform Module Remote Code	2023-10-10	7.0	High
CVE-2023-36718	products	Execution Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	Windows Container Manager Service Elevation of Privilege			
CVE-2023-36723	products	Vulnerability	2023-10-10	7.8	High
6) /5 2022 26725	microsoft - multiple	Mode a Karal Electron (De Bara) Incontilla	2022 40 40	7.0	112.1
CVE-2023-36725	products microsoft - multiple	Windows Kernel Elevation of Privilege Vulnerability Windows Internet Key Exchange (IKE) Extension Elevation of	2023-10-10	7.8	High
CVE-2023-36726	products	Privilege Vulnerability	2023-10-10	7.8	High
	microsoft - multiple				
CVE-2023-36729	products	Named Pipe File System Elevation of Privilege Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	Microsoft ODBC Driver for SQL Server Remote Code Execution			_
CVE-2023-36730	products	Vulnerability	2023-10-10	7.8	High
CVE-2023-36731	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
<u> </u>	microsoft - multiple	viniozic Elevation of Frivinege value (asime)	2023 10 10	7.0	111811
CVE-2023-36732	products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
	microsoft -				
CVE 2022 26727	azure_network_wa	Azure Network Watcher VM Agent Elevation of Privilege	2022 40 40	7.0	11: -l-
CVE-2023-36737	tcher microsoft - multiple	Vulnerability	2023-10-10	7.8	High
CVE-2023-36743	products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
	microsoft - multiple	Microsoft ODBC Driver for SQL Server Remote Code Execution			- 0
CVE-2023-36785	products	Vulnerability	2023-10-10	7.8	High
0.45 0000 0000	microsoft - multiple	Windows RDP Encoder Mirror Driver Elevation of Privilege			
CVE-2023-36790	products	Vulnerability Windows Client Server Bun time Subsystem (CSBSS) Floration of	2023-10-10	7.8	High
CVE-2023-41766	microsoft - multiple products	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability	2023-10-10	7.8	High
212 2020 12700	microsoft - multiple	0,			
CVE-2023-41772	products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
		Adobe Photoshop versions 23.5.5 (and earlier) and 24.7 (and			
		earlier) are affected by an Access of Uninitialized Pointer			
	adobe - multiple	vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user			
CVE-2023-26370	products	interaction in that a victim must open a malicious file.	2023-10-11	7.8	High
	p. 0 3 3 0 0	In temp_residency_name_store of thermal_metrics.c, there is a			
		possible out of bounds write due to a missing bounds check. This			
		could lead to local escalation of privilege with no additional			
CVE 2022 404 44	google ondered	execution privileges needed. User interaction is not needed for	2022 40 44	7.0	Lliah
CVE-2023-40141	google - android	exploitation. In TBD of TBD, there is a possible way to bypass carrier restrictions	2023-10-11	7.8	High
		due to a logic error in the code. This could lead to local escalation			
		of privilege with no additional execution privileges needed. User			
CVE-2023-40142	google - android	interaction is not needed for exploitation.	2023-10-11	7.8	High
		there is a possible use-after-free write due to improper locking.			
		This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for			
CVE-2023-3781	google - android	exploitation.	2023-10-11	7.8	High
	zabbix - multiple	The zabbix/src/libs/zbxjson module is vulnerable to a buffer	· · · · · · · · · · · · · · · · · · ·		
CVE-2023-32722	products	overflow when parsing JSON files via zbx_json_open.	2023-10-12	7.8	High
		SnapCenter versions 4.8 through 4.9 are susceptible to a			
CVE-2023-27316	netapp - snapcenter	vulnerability which may allow an authenticated SnapCenter Server user to	2023-10-12	7.8	High
<u> </u>	Shapeenter	1	-020 10 12	7.0	1 11611

		become an admin user on a remote system where a SnapCenter plug-in has been installed.			
		An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS allows an unauthenticated attacker with local access to the device to create a backdoor with root privileges. The issue is caused by improper directory permissions on a certain system directory, allowing an attacker with access to this directory to create a backdoor with root privileges.			
		This issue affects Juniper Networks Junos OS:			
		* All 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-S1.			
CVE-2023-44194	juniper - multiple products		2023-10-13	7.8	High
CVE-2023-43079	dell - emc_openmanage_ server_administrat or	Dell OpenManage Server Administrator, versions 11.0.0.0 and prior, contains an Improper Access Control vulnerability. A local low-privileged malicious user could potentially exploit this vulnerability to execute arbitrary code in order to elevate privileges on the system. Exploitation may lead to a complete system compromise.	2023-10-13	7.8	High
<u>CVE-2025-45079</u>	Ol	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading	2025-10-15	7.8	підіі
CVE-2023-35024	ibm - multiple products	to credentials disclosure within a trusted session. IBM X-Force ID: 258349.	2023-10-14	7.6	High
CVE-2023-40632	google - android	In jpg driver, there is a possible use after free due to a logic error. This could lead to remote information disclosure no additional execution privileges needed SAP PowerDesigner Client - version 16.7, does not sufficiently validate BPMN2 XML document imported from an untrusted	2023-10-08	7.5	High
CVE-2023-40310	sap - powerdesigner	source. As a result, URLs of external entities in BPMN2 file, although not used, would be accessed during import. A successful attack could impact availability of SAP PowerDesigner Client. When a client-side HTTP/2 profile and the HTTP MRF Router	2023-10-10	7.5	High
CVE-2023-40534	f5 - multiple products	option are enabled for a virtual server, and an iRule using the HTTP_REQUEST event or Local Traffic Policy are associated with the virtual server, undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	7.5	High
CVE-2023-40542	f5 - multiple products	When TCP Verified Accept is enabled on a TCP profile that is configured on a Virtual Server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2023-10-10	7.5	High
		When IPSec is configured on a Virtual Server, undisclosed traffic can cause TMM to terminate.			
CVE-2023-41085	f5 - multiple products	Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	7.5	High
<u>CVL-2023-41003</u>	citrix - multiple	Sensitive information disclosure in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA ?virtual?server.	2023-10-10	7.5	ı iigii
CVE-2023-4966	products	A very of CET was and worther both	2023-10-10	7.5	High
CVE-2023-37935	fortinet - multiple products	A use of GET request method with sensitive query strings vulnerability in Fortinet FortiOS 7.0.0 - 7.0.12, 7.2.0 - 7.2.5 and 7.4.0 allows an attacker to view plaintext passwords of remote services such as RDP or VNC, if the attacker is able to read the GET requests to those services.	2023-10-10	7.5	High
0.1 2020 37333	p. 044665	. 342330 13 1336 361 1.0031		,	۰۰۰۵۰۱

	for the sale	A interpretation conflict in Fortinet IPS Engine versions 7.321,			
CVE-2023-40718	fortinet - fortios_ips_engine	7.166 and 6.158 allows attacker to evade IPS features via crafted TCP packets.	2023-10-10	7.5	High
CVE-2023-29348	microsoft - multiple products	Windows Remote Desktop Gateway (RD Gateway) Information Disclosure Vulnerability	2023-10-10	7.5	High
CVE-2023-36431	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36435	microsoft - multiple products	Microsoft QUIC Denial of Service Vulnerability	2023-10-10	7.5	High
	microsoft - multiple				_
CVE-2023-36438	products microsoft - multiple	Windows TCP/IP Information Disclosure Vulnerability Windows Deployment Services Information Disclosure	2023-10-10	7.5	High
CVE-2023-36567	products microsoft - multiple	Vulnerability	2023-10-10	7.5	High
CVE-2023-36579	products microsoft - multiple	Microsoft Message Queuing Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36581	products	Microsoft Message Queuing Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36585	microsoft - multiple products	Active Template Library Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36596	microsoft - multiple products	Remote Procedure Call Information Disclosure Vulnerability	2023-10-10	7.5	High
CVE-2023-36602	microsoft - multiple products	Windows TCP/IP Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36603	microsoft - multiple products	Windows TCP/IP Denial of Service Vulnerability	2023-10-10	7.5	High
	microsoft - multiple				_
CVE-2023-36606	products microsoft - multiple	Microsoft Message Queuing Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36703	products microsoft - multiple	DHCP Server Service Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36707	products microsoft - multiple	Windows Deployment Services Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36709	products	Microsoft AllJoyn API Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36720	microsoft - multiple products	Windows Mixed Reality Developer Tools Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-38171	microsoft - multiple products	Microsoft QUIC Denial of Service Vulnerability	2023-10-10	7.5	High
		Incomplete Cleanup vulnerability in Apache Tomcat.			
		The internal fork of Commons FileUpload packaged with Apache Tomcat 9.0.70 through 9.0.80 and 8.5.85 through 8.5.93 included			
		an unreleased,			
		in progress refactoring that exposed a potential denial of service on			
		Windows if a web application opened a stream for an uploaded file but			
		failed to close the stream. The file would never be deleted from disk			
		creating the possibility of an eventual denial of service due to the disk being full.			
CVE-2023-42794	apache - multiple	Users are recommended to upgrade to version 9.0.81 onwards or	2023-10-10	7 5	⊔iah
CVL-2023-42/94	products	8.5.94 onwards, which fixes the issue. Vulnerability of package names' public keys not being verified in	7073-10-10	7.5	High
CVE-2023-44093	huawei - multiple products	the security module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
	huawei - multiple	Vulnerability of brute-force attacks on the device authentication module. Successful exploitation of this vulnerability may affect			
CVE-2023-44096	products huawei - multiple	service confidentiality. Clone vulnerability in the huks ta module. Successful exploitation of	2023-10-11	7.5	High
CVE-2023-44109	products	this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
	huawei - multiple	Use-After-Free (UAF) vulnerability in the surfaceflinger module.Successful exploitation of this vulnerability can cause			
<u>CVE-2023-44095</u>	products	system crash. Vulnerability of the permission to access device SNs being	2023-10-11	7.5	High
CVE-2023-44097	huawei - multiple products	improperly managed. Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
	huawei - multiple	Broadcast permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability may affect			J.:
CVE-2023-44100	products	service confidentiality.	2023-10-11	7.5	High
	huawei - multiple	The Bluetooth module has a vulnerability in permission control for broadcast notifications. Successful exploitation of this vulnerability			
<u>CVE-2023-44101</u>	products	may affect confidentiality. Out-of-bounds read vulnerability in the Bluetooth	2023-10-11	7.5	High
CVE-2023-44103	huawei - multiple products	module.Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
	huawei - multiple	Broadcast permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability may affect			G -7
CVE-2023-44104	products	service confidentiality.	2023-10-11	7.5	High

CVE-2023-44111	huawei - multiple products	Vulnerability of brute-force attacks on the device authentication module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVL 2023 44111	huawei - multiple	Type confusion vulnerability in the distributed file module.Successful exploitation of this vulnerability may cause the	2023 10 11	7.5	111611
CVE-2023-44108	products huawei - multiple	device to restart. Out-of-bounds array vulnerability in the dataipa module.Successful	2023-10-11	7.5	High
CVE-2023-44114	products	exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVE-2023-44119	huawei - multiple products	Vulnerability of mutual exclusion management in the kernel module. Successful exploitation of this vulnerability will affect availability. In ProtocolEmergencyCallListIndAdapter::Init of protocolcalladapter.cpp, there is a possible out of bounds read	2023-10-11	7.5	High
		due to a missing bounds check. This could lead to remote information disclosure with baseband firmware compromise			
CVE-2023-35652	google - android	required. User interaction is not needed for exploitation. In ProfSixDecomTcpSACKoption of RohcPacketCommon.cpp, there	2023-10-11	7.5	High
		is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not			
CVE-2023-35661	google - android	needed for exploitation.	2023-10-11	7.5	High
		An Improper Handling of Exceptional Conditions vulnerability in AS PATH processing of Juniper Networks Junos OS and Junos OS Evolved allows an attacker to send a BGP update message with an AS PATH containing a large number of 4-byte ASes, leading to a Denial of Service (DoS). Continued receipt and processing of these BGP updates will create a sustained Denial of Service (DoS) condition.			
		This issue is hit when the router has Non-Stop Routing (NSR) enabled, has a non-4-byte-AS capable BGP neighbor, receives a BGP update message with a prefix that includes a long AS PATH containing large number of 4-byte ASes, and has to advertise the prefix towards the non-4-byte-AS capable BGP neighbor.			
		Note: NSR is not supported on the SRX Series and is therefore not affected by this vulnerability. This issue affects:			
		Juniper Networks Junos OS:			
		* All versions prior to 20.4R3-S8; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; * 22.4 versions prior to 22.4R2-S1, 22.4R3; * 23.2 versions prior to 23.2R2.			
		Juniper Networks Junos OS Evolved			
		* All versions prior to 20.4R3-S8-EVO; * 21.1 versions 21.1R1-EVO and later; * 21.2 versions prior to 21.2R3-S6-EVO; * 21.3 versions prior to 21.3R3-S5-EVO; * 21.4 versions prior to 21.4R3-S5-EVO; * 22.1 versions prior to 22.1R3-S4-EVO; * 22.2 versions prior to 22.2R3-S2-EVO; * 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO; * 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO; * 23.2 versions prior to 23.2R2-EVO.			
	juniper - multiple				
CVE-2023-44186	products	ONTAP 9 versions prior to 9.8P19, 9.9.1P16, 9.10.1P12, 9.11.1P8,	2023-10-11	7.5	High
CVE-2023-27314	netapp - multiple products	9.12.1P2 and 9.13.1 are susceptible to a vulnerability which could allow	2023-10-12	7.5	High

		a remote unauthenticated attacker to cause a crash of the HTTP			
		service.			
		An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows a unauthenticated network-based attacker to cause an infinite loop, resulting in a Denial of Service (DoS).			
		An attacker who sends malformed TCP traffic via an interface configured with PPPoE, causes an infinite loop on the respective PFE. This results in consuming all resources and a manual restart is needed to recover.			
		This issue affects interfaces with PPPoE configured and tcp-mss enabled.			
		This issue affects Juniper Networks Junos OS			
		* All versions prior to 20.4R3-S7; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; * 22.4 versions prior to 22.4R2;			
CVE-2023-36841	juniper - multiple products		2023-10-12	7.5	High
		An Improper Handling of Inconsistent Special Elements vulnerability in the Junos Services Framework (jsf) module of Juniper Networks Junos OS allows an unauthenticated network based attacker to cause a crash in the Packet Forwarding Engine (pfe) and thereby resulting in a Denial of Service (DoS).			
		Upon receiving malformed SSL traffic, the PFE crashes. A manual restart will be needed to recover the device.			
		This issue only affects devices with Juniper Networks Advanced Threat Prevention (ATP) Cloud enabled with Encrypted Traffic Insights (configured via 'security-metadata-streaming policy').			
		This issue affects Juniper Networks Junos OS:			
		* All versions prior to 20.4R3-S8, 20.4R3-S9; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2-S1, 22.4R3;			
CVE-2023-36843	juniper - multiple products		2023-10-12	7.5	High
		A Reachable Assertion vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows to send specific genuine PIM packets to the device resulting in rpd to crash causing a Denial of Service (DoS).			
		Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition.			
	juniper - multiple	Note: This issue is not noticed when all the devices in the network are Juniper devices.			
CVE-2023-44175	products	This issue affects Juniper Networks:	2023-10-12	7.5	High

		T	T		T
		Junos OS:			
		* All versions prior to 20.4R3-S7; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R3; * 22.4 versions prior to 22.4R3.			
		Junos OS Evolved:			
		* All versions prior to 22.3R3-EVO; * 22.4-EVO versions prior to 22.4R3-EVO; * 23.2-EVO versions prior to 23.2R1-EVO.			
		An Improperly Implemented Security Check for Standard vulnerability in storm control of Juniper Networks Junos OS QFX5k devices allows packets to be punted to ARP queue causing a I2 loop resulting in a DDOS violations and DDOS syslog.			
		This issue is triggered when Storm control is enabled and ICMPv6 packets are present on device.			
		This issue affects Juniper Networks:			
		Junos OS			
		* All versions prior to 20.2R3-S6 on QFX5k; * 20.3 versions prior to 20.3R3-S5 on QFX5k; * 20.4 versions prior to 20.4R3-S5 on QFX5k; * 21.1 versions prior to 21.1R3-S4 on QFX5k; * 21.2 versions prior to 21.2R3-S3 on QFX5k; * 21.3 versions prior to 21.3R3-S2 on QFX5k; * 21.4 versions prior to 21.4R3 on QFX5k; * 22.1 versions prior to 22.1R3 on QFX5k; * 22.2 versions prior to 22.2R2 on QFX5k.			
CVF 2022 44404	juniper - multiple		2022 40 42	7.5	Hiah
CVE-2023-44181	products	An Improper Input Validation vulnerability in the routing protocol daemon (rpd) of Juniper Networks allows an attacker to cause a Denial of Service (DoS)to the device upon receiving and processing a specific malformed ISO VPN BGP UPDATE packet.	2023-10-13	7.5	High
		Continued receipt of this packet will cause a sustained Denial of Service condition.			
		This issue affects:			
		 * Juniper Networks Junos OS: * All 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 22.1R2-S2, 22.1R3; 			
CVE-2023-44185	juniper - multiple products	* 22.2 versions prior to 22.2R2-S1, 22.2R3; * 22.3 versions prior to 22.3R1-S2, 22.3R2.	2023-10-13	7.5	High

				1	
		# All versions prior to 20.4R3-S6-EVO; * 21.1-EVO version 21.1R1-EVO and later versions prior to 21.2R3-S4-EVO; * 21.3-EVO versions prior to 21.3R3-S3-EVO; * 21.4-EVO versions prior to 21.4R3-S3-EVO; * 22.1-EVO versions prior to 22.1R3-EVO; * 22.2-EVO versions prior to 22.2R2-S1-EVO, 22.2R3-EVO; * 22.3-EVO versions prior to 22.3R1-S2-EVO, 22.3R2-EVO.			
		An Allocation of Resources Without Limits or Throttling vulnerability in Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On all Junos OS QFX5000 Series and EX4000 Series platforms, when a high number of VLANs are configured, a specific DHCP packet will cause PFE hogging which will lead to dropping of socket connections. This issue affects:			
		<pre># 21.1 versions prior to 21.1R3-S5; # 21.2 versions prior to 21.2R3-S5; # 21.3 versions prior to 21.3R3-S5; # 21.4 versions prior to 21.4R3-S4; # 22.1 versions prior to 22.1R3-S3; # 22.2 versions prior to 22.2R3-S1; # 22.3 versions prior to 22.3R2-S2, 22.3R3; # 22.4 versions prior to 22.4R2.</pre>			
CVE-2023-44191	juniper - multiple products	This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1	2023-10-13	7.5	High
		An Improper Input Validation vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause memory leak, leading to Denial of Service (DoS). On all Junos OS QFX5000 Series platforms, when pseudo-VTEP (Virtual Tunnel End Point) is configured under EVPN-VXLAN scenario, and specific DHCP packets are transmitted, DMA memory leak is observed. Continuous receipt of these specific DHCP packets will cause memory leak to reach 99% and then cause the protocols to stop working and traffic is impacted, leading to Denial of Service (DoS) condition. A manual reboot of the system recovers from the memory leak. To confirm the memory leak, monitor for "sheaf:possible leak" and "vtep not found" messages in the logs. This issue affects: Juniper Networks Junos OS QFX5000 Series:			
CVE-2023-44192	juniper - multiple products	* All versions prior to 20.4R3-S6; * 21.1 versions prior to 21.1R3-S5;	2023-10-13	7.5	High

* 21.2 versions prior to 21.2R3-55; * 21.3 versions prior to 21.3R3-54; * 21.4 versions prior to 21.4R3-53; * 22.1 versions prior to 22.1R3-52; * 22.2 versions prior to 22.2R2-52, 22.2R3; * 22.3 versions prior to 22.2R2-51, 22.3R3; * 22.4 versions prior to 22.2R2-51, 22.3R3; * 22.4 versions prior to 22.4R1-52, 22.4R2. An Out-of-Bounds Write vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-58; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-52; * 21.3 versions prior to 21.4R3-55.
* 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R2-S2, 22.2R3; * 22.3 versions prior to 22.2R2-S2, 22.2R3; * 22.3 versions prior to 22.2R2-S1, 22.3R3; * 22.4 versions prior to 22.4R1-S2, 22.4R2. An Out-of-Bounds Write vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
* 22.3 versions prior to 22.3R2-S1, 22.3R3; * 22.4 versions prior to 22.4R1-S2, 22.4R2. An Out-of-Bounds Write vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configer with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.2R3-S5;
An Out-of-Bounds Write vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.2R3-S5;
Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
On all Junos OS and Junos OS Evolved devices an rpd crash and restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
restart can occur while processing BGP route updates received over an established BGP session. This specific issue is observed for BGP routes learned via a peer which is configured with a BGP import policy that has hundreds of terms matching IPv4 and/or IPv6 prefixes. This issue affects Juniper Networks Junos OS: * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
* All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
* 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
* 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
* 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3-S5;
* 21.3 versions prior to 21.3R3-S5;
1 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1
21.4 Versions prior to 21.4 N2 31, 21.4 N3 33.
This issue affects Juniper Networks Junos OS Evolved:
* All versions prior to 20.4R3-S8-EVO;
* 21.1-EVO version 21.1R1-EVO and later versions; * 21.2-EVO versions prior to 21.2R3-S2-EVO;
* 21.3-EVO version 21.3R1-EVO and later versions; * 21.4-EVO versions prior to 21.4R2-S1-EVO, 21.4R3-S5-EVO.
21.4-LVO Versions prior to 21.4N2-31-LVO, 21.4N3-33-LVO.
juniper - multiple
An Improper Check for Unusual or Exceptional Conditions
vulnerability in the SIP ALG of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated network-based attacker to cause an integrity impact in connected networks.
If the SIP ALG is configured and a device receives a specifically
malformed SIP packet, the device prevents this packet from being forwarded, but any subsequently received retransmissions of the same packet are forwarded as if they were valid.
This issue affects Juniper Networks Junos OS on SRX Series and MX
Series:
* 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-S1, 22.2R3;
* 22.3 versions prior to 22.3R1-S2, 22.3R2.
juninor multiple
juniper - multiple 2023-44198 T.5 High

		This issue doesn't not affected releases prior to 20.4R1.			
		An Improper Check for Unusual or Exceptional Conditions			
		vulnerability in the Packet Forwarding Engine (PFE) of Juniper			
		Networks Junos OS on MX Series allows a network-based,			
		unauthenticated attacker to cause a Denial of Service (DoS).			
		On Junos MX Series platforms with Precision Time Protocol (PTP)			
		configured, a prolonged routing protocol churn can lead to an FPC			
		crash and restart.			
		This issue affects Juniper Networks Junos OS on MX Series:			
		This issue affects jumper Networks Junos OS off Mix Series.			
		* All versions prior to 20.4R3-S4;			
		* 21.1 version 21.1R1 and later versions;			
		* 21.2 versions prior to 21.2R3-S2;			
		* 21.3 versions prior to 21.3R3-S5;			
		* 21.4 versions prior to 21.4R3;			
		* 22.1 versions prior to 22.1R3;			
		* 22.2 versions prior to 22.2R1-S1, 22.2R2.			
	juniper - multiple				
CVE-2023-44199	products		2023-10-13	7.5	High
		Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and			
		earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are			
		affected by an Improper Authorization vulnerability that could lead			
		in a security feature bypass in a way that an attacker could access			
0.45 0000 0000	adobe - multiple	unauthorised data. Exploitation of this issue does not require user			
CVE-2023-38220	products	interaction.	2023-10-13	7.5	High
		A improper limitation of a pathname to a restricted directory ('path traversal') in Fortinet FortiSandbox version 4.4.0 and 4.2.0			
		through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0 through 3.2.4 and			
	fortinet - multiple	2.5.0 through 2.5.2 and 2.4.1 and 2.4.0 allows attacker to denial of			
CVE-2023-41682	products	service via crafted http requests.	2023-10-13	7.5	High
072 2020 11002	products	A potential security vulnerability has been identified in the HP	2023 10 10	7.5	6
		ThinUpdate utility (also known as HP Recovery Image and			
		Software Download Tool) which may lead to information			
		disclosure. HP is releasing mitigation for the potential			
CVE-2023-4499	hp - thinupdate	vulnerability.	2023-10-13	7.5	High
		A path traversal vulnerability has been reported to affect several			
		QNAP operating system versions. If exploited, the vulnerability			
		could allow users to read the contents of unexpected files and			
		expose sensitive data via a network.			
		We have already fixed the vulnerability in the following versions:			
		QTS 5.1.0.2444 build 20230629 and later			
	qnap - multiple	QuTS hero h5.1.0.2424 build 20230609 and later			
CVE-2023-32974	products	QuTScloud c5.1.0.2498 and later	2023-10-13	7.5	High
		IBM Security Directory Server 6.4.0 could allow a remote attacker			
	ibm -	to traverse directories on the system. An attacker could send a			
01/5 0000 55	security_directory_	specially-crafted URL request containing "dot dot" sequences (//)	2225	_ =	
CVE-2022-33165	integrator	to view arbitrary files on the system. IBM X-Force ID: 228582.	2023-10-14	7.5	High
	ibm -	IBM Security Verify Access OIDC Provider could allow a remote user to cause a denial of service due to uncontrolled resource			
CVE-2022-43740	security_verify_acc ess_oidc_provider	consumption. IBM X-Force ID: 238921.	2023-10-14	7.5	High
CVL 2022-43/40	css_olac_provider	IBM QRadar SIEM 7.5.0 uses weaker than expected cryptographic	2023-10-14	ر. ،	iligii
	ibm - multiple	algorithms that could allow an attacker to decrypt highly sensitive			
CVE-2023-30994	products	information. IBM X-Force ID: 254138	2023-10-14	7.5	High
		An issue was discovered in drivers/usb/storage/ene_ub6250.c for			
		the ENE UB6250 reader driver in the Linux kernel before 6.2.5. An			
CVE-2023-45862	linux - linux_kernel	object could potentially extend beyond the end of an allocation.	2023-10-14	7.5	High
		The BIG-IP SPK TMM (Traffic Management Module) f5-debug-			
		sidecar and f5-debug-sshd containers contains hardcoded			
	fc h:~	credentials that may allow an attacker with the ability to intercept			
	f5 - big-	traffic to impersonate the SPK Secure Shell (SSH) server on those containers. This is only exposed when ssh debug is enabled. Note:			
	<pre>ip_next_service_pr oxy_for_kubernete</pre>	Software versions which have reached End of Technical Support			
CVE-2023-45226	S	(EoTS) are not evaluated	2023-10-10	7.4	High
	microsoft - multiple	,		<u> </u>	
CVE-2023-36561	products	Azure DevOps Server Elevation of Privilege Vulnerability	2023-10-10	7.3	High
	microsoft - multiple				
CVE-2023-36570	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
·		· · · · · · · · · · · · · · · · · · ·		_	

CVE-2023-35573 products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 7.3 High		microsoft - multiple				
CVE-2013-18572	CVE-2023-36571	•	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CFF-2023-36574	CVE-2023-36572	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
Microsoft Message Queuing Remote Code Secution Vulnerability 2023-10-10 7.3 High	CVE-2023-36573	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE_2023-36578	CVE-2023-36574	•	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 7,3 High	CVE-2023-36575	<u>'</u>	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 7.3 High	CVE-2023-36578	· ·	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
		microsoft - multiple				_
CVE_2023_36590 microsoft -multiple products Microsoft Message Queuing Remote Code Execution Vulnerability 2023_10_10 7.3 High		microsoft - multiple				_
Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High When a non-admin user has been assigned an administrator role via an iControl REST Put request and later the user's role is reverted back to a non-admin user has been assigned an administrator role via an iControl REST Put request and later the user's role is reverted back to a non-admin user has been assigned an administrator role via an iControl REST Put request and later the user's role is reverted back to a non-admin user can still have access to Control REST Put request and later the user's role is reverted back to a non-admin user can still have access to Control REST Put request and later for the products of Execution Vulnerability 2023-10-10 7.2 High microsoft multiple products in several functions of Express modern files, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with System execution provileges needed. User interaction is not needed for exploitation. A buffer copy without checking size of input vulnerability in the following versions: QTS 5.0.2445 build 20230699 and later QUTS here of S.0.2255 build 20230699 and later QUTS here of S.0.2255 build 20230699 and later QUTS here of S.0.2255 build 20230699 and later QUTS her		microsoft - multiple				
CVE-2023-36593 microsoft -multiple products microsoft multiple products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High When a non-admin user has been assigned an administrator role via an iControl REST PUT request and later the user's role is reverted back to a non-admin role via the Configuration utility. CVE-2023-36593 microsoft multiple products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-30 7.3 High When a non-admin user has been assigned an administrator role via an iControl REST PUT request and later the user's role is reverted back to a non-admin role via the Configuration utility. CVE-2023-36786 fis-multiple products microsoft multiple products microsoft multiple products microsoft multiple products microsoft multiple products when the control REST Put request and later the user's role is reverted back to a non-admin user has been assigned an administrator role via an iControl REST RUT request and later the user's role is reverted back to a non-admin user can still have access to iControl REST Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple products increased find of Technical Support (EdTS) are not evaluated. 2023-10-10 7.2 High microsoft multiple products in several functions of Exproso modern files, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. VVF-2023-35649 google - android University in the Collowing system versions: If exploited, the university in the following versions: Control of REST Supported to affect several QNAP operating system versions: If exploited, the university in the following versions: Container Station of Collowing System versions: If exploited, the university in the following versions: Container Station of Collowing System versions: Con	CVE-2023-36589		Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 7.3 High	CVE-2023-36590	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 7.3 High microsoft multiple products Microsoft Message Queuing Remote Code Execution Vulnerability 2023-10-10 7.3 High	CVE-2023-36591	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
When a non-admin user has been assigned an administrator role via an Kontrol REST PUT request and later the user's role is reverted back to a non-admin role via the Configuration utility, trash, or 'Cinotrol REST BIG-Pi moral administrator role via the Configuration utility, trash, or 'Cinotrol REST BIG-Pi moral administrator role via the Configuration utility, trash, or 'Cinotrol REST BIG-Pi moral administration user can still have access to iControl REST administed resource. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. VE-2023-36780 microsoft - multiple products When a non-admin role via the Configuration utility, trash, or 'Cinotrol REST administrators to de Execution Vulnerability VE-2023-36780 microsoft - multiple products Skype for Business Remote Code Execution Vulnerability VE-2023-36780 microsoft - multiple products In several functions of Exynos modern files, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. VE-2023-35649 google - android VE-2023-35640 google - android VE-2023-35650 google - android VE-2023-36560 google - android VE-2023-36560 google - andr	CVE-2023-36592	products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
via an iControl REST PUT request and later the user's fole is reverted back to a non-admin role via the Configuration utility, trish, or iControl REST Mills Gentlement of the Configuration utility, trish, or iControl REST Mills resource. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. VE-2023-36780 microsoft - multiple products microsoft - multiple microsoft - multiple products microsoft - multiple product	CVE-2023-36593	· ·	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
reverted back to a non-admin role via the Configuration utility, tmsh, or Control REST, Bid-P non-admin user can still have access to iControl REST admin resource. Note: Software versions which products between the products microsoft - multiple p						
trish, or IControl REST. BIG-IP non-admin user can still have access to products in control REST and in resource. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. VE-2023-36789 microsoft - multiple products of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. VE-2023-35649 google - android User interaction is not needed for exploitation. A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2435 build 20230699 and later QUTS hero h5.1.0.2444 build 20230791 and later QUTS hero h5.1.0.2444 build 20230791 and later QUTS hero h5.1.0.2435 build 20230793 and later QUTS hero h5.1.0.2436 build 20230793 and later			· ·			
weight w			· · · ·			
Microsoft multiple products Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple products Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft multiple 2023-10-10 7.1 High microsoft multiple 2023-10	CVE 2022 42769	•		2022 10 10	7.2	Hiah
CVE-2023-36786 products produc		microsoft - multiple				
Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-11 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-11 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-11 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-11 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-11 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-11 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-13 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-13 7.2 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple Skype for Business Remote Code Execution Vulnerability 2023-10-10 7 High mic	CVE-2023-36780	· ·	Skype for Business Remote Code Execution Vulnerability	2023-10-10	7.2	High
Sykpe for Business Remote Code Execution Vulnerability 2023-10-10 7.2 High In several functions of Expross modern files, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. System interaction is not needed for exploitation. A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2445 build 20230599 and later QTS 4.5.4.2467 build 20230599 and later QUTS hero h5.1.0.2444 build 20230699 and later QUTS hero h5.1.0.2442 build 20230690 and later QUTS hero h5.1.0.2444 build 20230690 and later QUTS hero h5.1.0.2442 build 20230690 and later QUTS hero h5.1.0.2498 and later QUTS hero h5.1.0.2442 build 20230690 and later QUTS hero h5.1.0.2452 build 20230690 and later QUTS hero h5.1.0.2452 build 20230690 build	CVE-2023-36786	products	Skype for Business Remote Code Execution Vulnerability	2023-10-10	7.2	High
of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation. A buffer copy without checking size of input vulnerability has been reported to affect everal QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.12425 build 20230609 and later QTS hero h5.10.2434 build 20230609 and later QTS hero h5.10.2434 build 202309078 and later QUTS hero h5.10.2438 and later QUTS hero h5.10.2438 and later QUTS hero h5.10.2438 and later QUTS hero h5.10.2448 build 20230728 and later QUTS hero h5.10.2438 and later QUTS hero h5.10.2448 and later QUTS hero h5.10.24748 and later QUTS hero h4.5.4.2476 build 20230728 and later QUTS hero h5.10.24748 and	CVE-2023-36789	· ·		2023-10-10	7.2	High
QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 2023073 and later QuTS hero h5.0.1.2515 build 20230728 and later QuTS hero h5.10.2424 build 20230728 and later QUTS hero h5.10.2424 build 20230728 and later QUTS hero h4.5.4.2476 build 20230728 and later An OS command injection vulnerability could allow authenticated administrators to execute commands via a network. We have already fixed the vulnerability outlous via a network. We have already fixed the vulnerability in the following version: Container station 2.6.7.44 and later An improper neutralization of special elements used in an os command ('os command injection') in FortiManager 7.4.0 and 7.2.0 through 7.2.3 may allow attacker to execute unauthorized code or commands via FortiManager cli. Wicrosoft - multiple products microsoft - multiple products microsoft - multiple products microsoft - multiple vulnerability v	CVE-2023-35649	google - android	of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation. A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated	2023-10-11	7.2	High
CVE-2023-32976 container_station	CVE-2023-32973	products	QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.0.2424 build 20230609 and later QuTS hero h4.5.4.2476 build 20230728 and later QuTScloud c5.1.0.2498 and later An OS command injection vulnerability has been reported to affect Container Station. If exploited, the vulnerability could allow authenticated administrators to execute commands via a network.	2023-10-13	7.2	High
command ('os command injection') in FortiManager 7.4.0 and 7.2.0 through 7.2.3 may allow attacker to execute unauthorized code or commands via FortiManager cli. microsoft - multiple products microsoft - multiple products Microsoft Office Graphics Elevation of Privilege Vulnerability CVE-2023-36568 products Microsoft Office Click-To-Run Elevation of Privilege Vulnerability CVE-2023-36568 microsoft - multiple products Microsoft Office Click-To-Run Elevation of Privilege Vulnerability CVE-2023-36721 products Microsoft Office Click-To-Run Elevation of Privilege Vulnerability CVE-2023-36721 products Mindows Error Reporting Service Elevation of Privilege Vulnerability CVE-2023-36776 microsoft - multiple products Mindows Runtime Remote Code Execution Vulnerability Mindows Runtime Remote Code Execution Vu	CVE-2023-32976		Container Station 2.6.7.44 and later	2023-10-13	7.2	High
CVE-2023-36565productsMicrosoft Office Graphics Elevation of Privilege Vulnerability2023-10-107HighCVE-2023-36568productsMicrosoft Office Click-To-Run Elevation of Privilege Vulnerability2023-10-107HighMicrosoft - multiple productsWindows Error Reporting Service Elevation of Privilege2023-10-107HighMicrosoft - multiple productsVulnerability2023-10-107HighCVE-2023-36776productsWin32k Elevation of Privilege Vulnerability2023-10-107HighCVE-2023-36902productsWindows Runtime Remote Code Execution Vulnerability2023-10-107Highmicrosoft - multiple microsoft - multiplemicrosoft - multiple44	CVE-2023-41838	products	command ('os command injection') in FortiManager 7.4.0 and 7.2.0 through 7.2.3 may allow attacker to execute unauthorized	2023-10-10	7.1	High
microsoft - multiple products Microsoft Office Click-To-Run Elevation of Privilege Vulnerability 2023-10-10 7 High microsoft - multiple products Vulnerability Vulnerability 2023-10-10 7 High microsoft - multiple products Win32k Elevation of Privilege Vulnerability 2023-10-10 7 High microsoft - multiple products Win32k Elevation of Privilege Vulnerability 2023-10-10 7 High microsoft - multiple products Windows Runtime Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple products Windows Runtime Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple	CVE-2023-36565	•	Microsoft Office Graphics Elevation of Privilege Vulnerability	<u>2</u> 023-10-10	7	High
microsoft - multiple products Vulnerability 2023-10-10 7 High CVE-2023-36721 products Vulnerability 2023-10-10 7 High CVE-2023-36776 products Win32k Elevation of Privilege Vulnerability 2023-10-10 7 High CVE-2023-36902 products Windows Runtime Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple products Windows Runtime Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple		microsoft - multiple		2023-10-10	7	
CVE-2023-36776 microsoft - multiple products Win32k Elevation of Privilege Vulnerability 2023-10-10 7 High microsoft - multiple products Windows Runtime Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple		microsoft - multiple	Windows Error Reporting Service Elevation of Privilege			_
microsoft - multiple products Windows Runtime Remote Code Execution Vulnerability 2023-10-10 7 High microsoft - multiple		microsoft - multiple				
microsoft - multiple		microsoft - multiple	-			_
THE COLUMN TO MICHIGAN TO AN INCLUSION OF THE PROPERTY OF THE	CVE-2023-38159	· ·	Windows Graphics Component Elevation of Privilege Vulnerability	2023-10-10	7	High

	lenovo -	A vulnerability was reported in ThinkPad T14s Gen 3 and X13 Gen3 that could cause the BIOS tamper detection mechanism to not			
CVE-2022-3728	thinkpad_t14s_gen _3_firmware	trigger under specific circumstances which could allow unauthorized access.	2023-10-09	6.8	Medium
CVE-2022-48182	lenovo - thinkpad_t14s_gen _3_firmware	A vulnerability was reported in ThinkPad T14s Gen 3 and X13 Gen3 that could cause the BIOS tamper detection mechanism to not trigger under specific circumstances which could allow unauthorized access.	2023-10-09	6.8	Medium
	lenovo -	A vulnerability was reported in ThinkPad T14s Gen 3 and X13 Gen3 that could cause the BIOS tamper detection mechanism to not			
CVE-2022-48183	thinkpad_t14s_gen _3_firmware	trigger under specific circumstances which could allow unauthorized access. Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and	2023-10-09	6.8	Medium
CVE-2023-26366	adobe - multiple products hp -	earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A high-privileged authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction, scope is changed due to the fact that an attacker can enforce file read outside the application's path boundary. HP is aware of a potential security vulnerability in HP t430 and t638 Thin Client PCs. These models may be susceptible to a physical attack, allowing an untrusted source to tamper with the system firmware using a publicly disclosed private key. HP is	2023-10-13	6.8	Medium
CVE-2023-5409	t430_thin_client_fir mware	providing recommended guidance for customers to reduce exposure to the potential vulnerability.	2023-10-13	6.8	Medium
<u> </u>	iliwale	In FW-PackageManager, there is a possible missing permission	2023 10-13	0.0	IVICUIUIII
CVE-2023-40653	google - android	check. This could lead to local escalation of privilege with System execution privileges needed In FW-PackageManager, there is a possible missing permission	2023-10-08	6.7	Medium
CVE-2023-40654	google - android	check. This could lead to local escalation of privilege with System execution privileges needed	2023-10-08	6.7	Medium
CVE-2023-37194	siemens - simatic_cp_1604_fi	A vulnerability has been identified in SIMATIC CP 1604 (All versions), SIMATIC CP 1616 (All versions), SIMATIC CP 1623 (All versions), SIMATIC CP 1626 (All versions), SIMATIC CP 1628 (All versions). The kernel memory of affected devices is exposed to user-mode via direct memory access (DMA) which could allow a local attacker with administrative privileges to execute arbitrary code on the host system without any restrictions.	2023-10-10	6.7	Medium
CVE-2023-37194	rmware	In ctrl_roi of stmvl53l1_module.c, there is a possible out of bounds	2025-10-10	6.7	ivieulum
CVE-2023-35654	google - android	read due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. In CanConvertPadV2Op of darwinn_mlir_converter_aidl.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local escalation of privilege with System	2023-10-11	6.7	Medium
CVE-2023-35655	google - android	execution privileges needed. User interaction is not needed for exploitation. In lwis_transaction_client_cleanup of lwis_transaction.c, there is a possible way to corrupt memory due to a use after free. This could	2023-10-11	6.7	Medium
CVE-2023-35660	google - android	lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and	2023-10-11	6.7	Medium
CVE-2023-38221	adobe - multiple products	earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead in arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction and attack complexity is high as it requires knowledge of tooling beyond just using the UI.	2023-10-13	6.6	Medium
<u> </u>	·	Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead in arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user	_523 10 13	3.0	caidiii
CVE-2023-38249	adobe - multiple products	interaction and attack complexity is high as it requires knowledge of tooling beyond just using the UI.	2023-10-13	6.6	Medium
		Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead in			
CVE-2023-38250	adobe - multiple products	arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user	2023-10-13	6.6	Medium

	sap -	interaction and attack complexity is high as it requires knowledge of tooling beyond just using the UI. SAP NetWeaver AS Java (GRMG Heartbeat application) - version 7.50, allows an attacker to send a crafted request from a			
CVE-2023-42477	netweaver_applicat ion_server_java	vulnerable web application, causing limited impact on confidentiality and integrity of the application.	2023-10-10	6.5	Medium
		The BIG-IP and BIG-IQ systems do not encrypt some sensitive information written to Database (DB) variables.			
	f5 - multiple	Note: Software versions which have reached End of Technical			
CVE-2023-41964	products	Support (EoTS) are not evaluated. A client-side enforcement of server-side security [CWE-602]	2023-10-10	6.5	Medium
		vulnerability in Fortinet FortiManager version 7.4.0 and before 7.2.3 and FortiAnalyzer version 7.4.0 and before 7.2.3 may allow a			
	fortinet - multiple	remote attacker with low privileges to access a privileged web			
CVE-2023-42787	products	console via client side code execution. An authorization bypass through user-controlled key [CWE-639]	2023-10-10	6.5	Medium
	fortinet - multiple	vulnerability in Fortinet FortiManager version 7.4.0 and before 7.2.3 and FortiAnalyzer version 7.4.0 and before 7.2.3 allows a remote attacker with low privileges to read sensitive information			
CVE-2023-44249	products	via crafted HTTP requests.	2023-10-10	6.5	Medium
CVE-2023-36429	microsoft - multiple products	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	2023-10-10	6.5	Medium
	microsoft - multiple	Microsoft Dynamics 365 (On-Premises) Information Disclosure			
CVE-2023-36433	products microsoft - multiple	Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36563	products	Microsoft WordPad Information Disclosure Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36564	microsoft - multiple products microsoft - multiple	Windows Search Security Feature Bypass Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36566	products	Microsoft Common Data Model SDK Denial of Service Vulnerability Windows Deployment Services Information Disclosure	2023-10-10	6.5	Medium
CVE-2023-36706	microsoft - multiple products	Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36717	microsoft - multiple products	Windows Virtual Trusted Platform Module Denial of Service Vulnerability	2023-10-10	6.5	Medium
	products	Inappropriate implementation in DevTools in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control		0.0	
CVE-2023-5475	google - chrome	via a crafted Chrome Extension. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
		Inappropriate implementation in Extensions API in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a			
CVE-2023-5479	google - chrome	crafted HTML page. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
		Inappropriate implementation in Downloads in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to spoof security			
CVE-2023-5481	google - chrome	UI via a crafted HTML page. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
		Inappropriate implementation in Intents in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to bypass content			
CVE-2023-5483	google - chrome	security policy via a crafted HTML page. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
<u> </u>	google ellione	Inappropriate implementation in Navigation in Google Chrome	2023 10 11	0.5	Wicaram
CVE-2023-5484	google - chrome	prior to 118.0.5993.70 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
		Inappropriate implementation in Fullscreen in Google Chrome prior to 118.0.5993.70 allowed an attacker who convinced a user			
		to install a malicious extension to bypass navigation restrictions via			
CVE-2023-5487	google - chrome	a crafted Chrome Extension. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
		·			
		A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS).			
		PTX3000, PTX5000, QFX10000, PTX1000, PTX10002, and PTX10004, PTX10008 and PTX10016 with LC110x FPCs do not			
		support certain flow-routes. Once a flow-route is received over an established BGP session and an attempt is made to install the resulting filter into the PFE, FPC heap memory is leaked. The FPC heap memory can be monitored using the CLI command "show chassis fpc".			
		The following syslog messages can be observed if the respective filter derived from a flow-route cannot be installed.			
CVE-2023-22392	juniper - multiple products	expr_dfw_sfm_range_add:661 SFM packet-length Unable to get a sfm entry for updating the hw	2023-10-12	6.5	Medium
CVL-2023-22332	Products	Jim Chay for apading the five		0.5	IVICUIUIII

exp_div_su_sin_addx.720 Lands to add the father second-investor to the areaware sequilibrium. Jour_addx.72 father to the areaware sequilibrium. Jour_addx.72 father to the second						
corp., div., base., bus., add.55 Palled to add hylv sist notes. expr., gife, base., bus., create-114 Failed to dail hylv sist notes. expr., gife, base., pic., create-114 Failed to create base inst for sitter to sit PE to J. (Covarse, circles), and judge control of the covarse. Linux, pic., called linux, and linux, an						
eyar_div_base_ple_inst_cream24 Failed to create that inst for shifter on PE to for_divoraget_claimst_inet_ crypt_claimst_inet_ crypt_claimst_inet_ and install_inet_ crypt_claimst_inet_ c						
stiller of on PPTG forlowspec_default_inet engr_dwlrinetchanges_adsFault_tesflowspec_default_tes on PPTG or engr_dwlrinetengr_flowr						
exer diffy ift, inst, change; 1868 Falled to create			· = = = = = = = = = =			
cyar div. No. pgm. flumo565 div. plc. jms. oli and trund for pier. index 0.1 cyar_div. bp. pgm. ll_mam.548 Failled to ggm blind-point in live generic failure corp. div. bp. tope. headder:130 Failed to grayum in tumo cyar_div. bp. tope. headder:130 Failed to thange instance for fifter. Inflowed cell-air. line: This bouse affects. Junipe. RVINO004, PIX10006 and PIX10016 with ICHION PICE: This bouse affects. Junipe. RVINO004, PIX10006 and PIX10016 with ICHION PICE: **All versions prior to 20.088-55; **2.11 versions prior to 20.088-55; **2.12 versions prior to 21.88-54; **2.12 versions prior to 21.88-52; **2.13 versions prior to 21.88-52; **2.14 versions prior to 21.88-53; **2.14 versions prior to 17.88-53; **2.14 versions prior to 17.88-53; **2.15 versions prior to 17.88-53; **2.14 versions prior to 17.88-53; **2.12 versions prior to 21.88-55; **2.13 versions prior to 21.88-55; **2.14 versions prior to 21.88-53; **2.12 versions prior to 21.88-53; **2.12 versions prior to 21.88-53; **2.12 versions prior to 22.88-53; **2.12 versions of and Juno 35 Siched allow an ununthenicated adjacent attacker who sends specific LIDP packets to cause a denied of Service due allow an ununthenicated adjacent attacker who sends specific LIDP packets to cause a denied of Service due allow an ununthenicated adjacent attacker who sends specific LIDP packets to cause a denied of Service due allow an ununthenicated adjacent attacker who sends specific LIDP packets to cause a denied of Service due allow an ununthenicated adjacent attacker who sends specific LIDP packets to cause a denied of Service due allow an ununthenicated adjacent attacker who sends specific LIDP packets are received and telementy solidies is being done on the device.			expr_dfw_flt_inst_change:1368 Failed to create			
ple_index OI exp_dw_bp_gmm ft_numS48 Failed to pgm bind-point in hw: generic failure exp_dw_bp_tooo_handler1102 Failed to program fnum. exp_dw_bp_tooo_handler1102 Failed to program fnum. exp_dw_bp_tooo_handler1102 Failed to program fnum. exp_dw_enity_process_dehan_enc3 This lose affects bursier. Review fs_buss OS: on PPA3000, PPA30002 and PPA100004, PPX10008 and PPX10016 with LC110x FPCs: * All versions prior to 20.489.55 * 2.1 symptom prior to 20.489.55 * 2.1 symptom prior to 21.483.42 * 2.2 versions prior to 21.483.22 * 2.2 versions prior to 22.481.52, 22.182, * 2.2 versions prior to 22.481.52, 22.182, * 2.3 versions prior to 22.483.55 * 3.1 symptom prior to 22.483.55 * 3.1 symptom prior to 24.483.55 * 3.1 symptom prior to 24.483.55 * 3.1 symptom prior to 22.483.55 * 3.1 symptom prior to 22.483.55 * 3.2 symptom prior to 22.483.55 * 3.3 symptom prior to 22.483.55 * 3.4 symptom prior to 22.483.55 * 3.5 symptom prior to 22.483.53 * 3.5 symptom prior to 22.485.55 * 3.6 symptom prior to 22.485.55 * 3.6 symptom prior to 22.485.55 * 3.7 symptom prior to 22.485.55 * 3.8 symptom prior to 22.485.55 * 3.9 symptom prior to 22.483.55 * 3.1 symptom prior to 22.483.55 * 3.1 symptom prior to 22.483.55 * 3.1 symptom prior to 22.483.55 * 3.2 symptom prior to 22.482.55 * 3.2 symp						
generic failure expt. (div. bp., topo, handlecis102 failed to program froum. sopt, div. entry, process, changes 679 Failed to change instance for filter						
expr. dfw. pd., Dop., handler:1102 Falled to program frum. copr. dfw. pd. process, default_inet This issue affects uniper Networks Junion OS: on PTX1000, PTX10002, and PTX10004, PTX10008 and PTX10016 with ICT104 FPCs: * All versions prior to 20.483-SS; * 7.1.1 versions prior to 17.183-S4; * 2.1.2 versions prior to 17.183-S4; * 2.1.3 versions prior to 17.183-S4; * 2.1.3 versions prior to 17.183-S4; * 2.1.3 versions prior to 17.183-S4; * 2.1.4 versions prior to 17.183-S4; * 2.1.4 versions prior to 17.183-S4; * 2.1.3 versions prior to 17.183-S4; * 2.1.3 versions prior to 20.483-S8; * 2.1.3 versions prior to 20.183-S5; * 2.1.4 versions prior to 20.183-S5; * 2.1.4 versions prior to 20.183-S5; * 2.1.3 versions prior to 20.183-S5; * 2.1.4 versions prior to 20.185-S4; * 2.1.3 versions prior to 20.185-S4; * 2.1.3 versions prior to 20.185-S4; * 2.1.4 versions prior to 20.183-S6; * 2.1.4 versio						
espc_effw_entry_process_change_eff9Fafied to change instance for filter_filter_filter_files_ched_efful_file This issue affects Juniper Networks Junos OS: on PTX0000, PTX00002, and PTX10004, PTX10008 and PTX10016 with LC110x PFX.: * All versions prior to 20.4R8-SS; * 21.1 versions prior to 21.88-S4; * 21.2 versions prior to 21.88-S4; * 21.3 versions prior to 22.4R1-S2, 22.4R3; * 22.1 versions prior to 22.4R2-S2, 22.4R3; * 22.1 versions prior to 22.4R3-S8; * 21.1 versions prior to 22.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 22.4R3-S8; * 21.3 versions prior to 22.4R3-S8; * 21.3 versions prior to 22.4R3-S8; * 21.3 versions prior to 22.4R3-S4; * 22.4 versions prior to 22.4R3-S4; * 22.4 versions prior to 22.4R3-S4; * 22.4 versions prior to 22.4R3-S4; * 22.2 versions prior to 22.4R3-S4; * 22.3 versions prior to 22.4R3-S4; * 22.4 versions prior to 22.4R3-S6; * 23.4 versions prior to 22.4R3-S6; * 24.4 versions prior to 22.4R3-S6; * 25.4 versions prior to 22.4R3-S6; * 26.4 versions prior to 22.4R3-S6; * 27.4 versions prior to 22.4R3-S6; * 27.5 versions prior to 22.4R3-S6; * 27.1 versions prior to 22.4R3-S6; * 27.2 versions						
This issue affects Juniper Networks Junos OSS on PTX1000, PTX10007, and PTX10008 and PTX10016 with ICL110x PCC: **All versions prior to 20.4R3-55; **21.1 versions prior to 20.4R3-55; **21.2 versions prior to 20.4R3-52, 22.4R3; **22.1 versions prior to 20.4R3-58; **21.1 versions prior to 20.4R3-58; **21.1 versions prior to 20.4R3-58; **21.1 versions prior to 20.4R3-55; **21.2 versions prior to 20.4R3-55; **22.3 versions prior to 20.4R3-55; **22.3 versions prior to 20.4R3-55; **22.4 versions prior to 20.4R3-56; **22.3 versions prior to 20.4R3-56; **22.4 versions prior to 20.4R3-56; **22.4 versions prior to 20.4R3-56; **23.4 versions prior to 20.4R3-56; **24.4 versions prior to 20.4R3-56; **25.5 versions prior to 20.4R3-56; **26.5 versions prior to 20.4R3-56; **27.4 versions prior to 20.4R3-56; **28.5 versions prior to 20.4R3-56; **29.5 versions prior to 20.4R3-56; **29.6 versions prior to 20.4R3-58; **29.7 versions prior to 20.4R3-58; **29.1 versions prior to 20.288-58; **29.29 versions prior to 20.288-58; **29.20 versions prior to 20.288-58; **29.20 versions						
on PTX10002, PTX10002, and PTX10004, PTX10008 and PTX10016 with LC110x FPCs: * All versions prior to 20.4R3-S5; * 21.1 versions prior to 21.4R3-S5; * 21.3 versions prior to 21.3R3.* * 21.4 versions prior to 21.3R3.* * 22.1 versions prior to 22.4R3-S2; * 21.1 versions prior to 22.4R3-S2; * 21.1 versions prior to 22.4R3-S2; * 21.1 versions prior to 22.4R3-S3; * 21.1 versions prior to 22.4R3-S3; * 21.1 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.2R3-S6; * 21.4 versions prior to 21.4R3-S4; * 21.1 versions prior to 21.4R3-S4; * 21.1 versions prior to 22.4R3-S4; * 21.2 versions prior to 22.4R3-S4; * 21.2 versions prior to 22.4R3-S4; * 21.2 versions prior to 22.4R3-S4; * 21.4 versions prior to 22.4R2. An improper Validation of Specified Quantity in input vulnerability in the Layer-2 control protocols daemon (Vcpql) of Jumper Networks Junos QS and Junos QS evolved allows an unautheritated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(FQS). This issue occurs when specific LLDP packets are received and telementry polling is being done on the delived. The impact of the Dayd crash is remitilatation of STP protocols fixTP, MSTP or QS and Packets of the Packets						
with LC1IDx FPCS: * All versions prior to 20.483-55; * 21.1 versions prior to 21.283-32; * 21.3 versions prior to 21.283-32; * 21.3 versions prior to 21.283-32; * 21.3 versions prior to 21.482-52, 21.483; * 21.4 versions prior to 21.482-53, 21.483; * 21.1 versions prior to 20.483-38; * 21.1 versions prior to 20.483-38; * 21.1 version prior to 21.283-36; * 21.3 versions prior to 21.283-36; * 21.3 versions prior to 21.283-36; * 21.3 versions prior to 21.383-35; * 21.4 versions prior to 21.383-35; * 21.4 versions prior to 21.283-33 * 22.4 versions prior to 22.282-32, 22.383 * 22.4 versions prior to 22.382-32, 22.383 * 22.4 versions prior to 22.482. An improper Validation of Specified Quantity in Input vulnerability in the Layer 2 control protocols deemon (Ecodi Of Juniper Networks) and unauthenticated adjacent attacker who sends specific LIDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry poiling is being done on the device. The impact of the Lipper cash is relatibilization of ST Protocols (ESTP, MSTP or VSTP), and MVMP and FRP. Also, if any services depend on LIDP state (Ike Pof or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.483-38; * 21.1 versions prior to 21.843-35; * 21.1 versions prior to 21.843-35; * 21.1 versions prior to 21.483-35; * 21.1 versions prior to 21.483-35; * 21.1 versions prior to 21.483-35; * 21.1 versions prior to 22.483-35; * 22.1 versions prior to 22.483-35; * 22.1 versions prior to 22.2843-35; * 22.2 versions prior to 22.2842-25; * 22.3 versions prior to 22.2842-25; * 22.3 versions prior to 22.2842-25; * 22.4 versions prior to 22.2842-25; * 22.3 versions prior to 22.2842-25; * 22.4 versions prior to 22.2842-25; * 22.5 versions prior to 22.2842-25; * 22.5 versions prior to 22.2842-25; *			This issue affects Juniper Networks Junos Os:			
* All versions prior to 20.483-55; * 2.1.1 versions prior to 21.183-34; * 2.1.2 versions prior to 21.283-32; * 2.1.3 versions prior to 21.283-32; * 2.1.4 versions prior to 21.283-32; * 2.1.4 versions prior to 22.181-52; 22.182; on PTX3000, PTX5000, QFX10000: * All versions prior to 22.181-52; 22.182. on PTX3000, PTX5000, QFX10000: * All versions prior to 22.183-36; * 2.1.4 versions prior to 21.283-36; * 2.2.4 versions prior to 22.283-2; * 2.2.4 versions prior to 22.283-2; * 22.4 versions prior to 22.882-2; * 22.4 versions prior to 22.883-3; * 21.1 version 23.882-3; * 21.1 version 23.882-3; * 21.1 version 23.883-3; * 21.1 version 23.883-3; * 21.1 version 24.283-3; * 22.1 version 25.883-3; * 22.1 version 25.283-3; * 22.2 versions prior to 22.283-3; * 22.2 versions prior to 22.283-3; * 22.2 versions prior to 22.283-3; * 22.3 versions prior to 22.282-2; * 22.3 versions prior to 22.282-2; * 22.3 versions prior to 22.282-2; * 22.3 versions prior to 22.242-2; * 22.4 versions prior to 22.242-2; * 22.3 versions prior to 22.242-2; * 22.4 versions prior to 22.242-2; * 22.3 versions prior to						
* 21.1 versions prior to 21.183-54; * 21.2 versions prior to 21.283-52; * 21.3 versions prior to 13.813; * 21.4 versions prior to 22.181-52, 22.14R3; * 22.1 versions prior to 22.181-52, 22.14R3; * 22.1 versions prior to 22.181-52, 22.182. on PTX3000, PTX5000, QFX10000: * All versions prior to 20.483-58; * 21.1 version 21.181 and later versions; * 21.1 version 21.181 and later versions; * 21.2 versions prior to 12.183-55; * 21.3 versions prior to 12.183-55; * 21.4 versions prior to 12.183-35; * 21.2 versions prior to 22.183-34 * 22.2 versions prior to 22.183-34 * 22.2 versions prior to 22.283-3 * 22.2 versions prior to 22.382-52, 22.383 * 22.2 versions prior to 22.482. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (12xpd) of Juniper Networks Junes OS and Junos OS Fovbed allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling its being done on the device. The impact of the Dzcpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVPP and LBPs. Alb, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS All versions prior to 20.483-58; * 21.1 versions prior to 21.383-54; * 21.2 versions prior to 21.383-54; * 21.4 versions prior to 21.483-33; * 22.1 versions prior to 22.482-53; * 22.2 versions prior to 22.482-53; * 22.3 versions prior to 22.483-53; * 22.4 versions prior to 22.483-53; * 22.5 versions prior to 22.483-53; * 22.5 versions prior to 22.483-53; * 22.6 versions prior to 22.483-53; * 22.7 versions prior to 22.483-53; * 22.8 versions prior to 22.483-53; * 22.9 versions prior to 22.4842-54; * 22.4 versions prior to 22.4842-54; * 22.5 versions prio			with LC110x FPCs:			
* 21.1 versions prior to 21.183-54; * 21.2 versions prior to 21.283-52; * 21.3 versions prior to 13.813; * 21.4 versions prior to 22.181-52, 22.14R3; * 22.1 versions prior to 22.181-52, 22.14R3; * 22.1 versions prior to 22.181-52, 22.182. on PTX3000, PTX5000, QFX10000: * All versions prior to 20.483-58; * 21.1 version 21.181 and later versions; * 21.1 version 21.181 and later versions; * 21.2 versions prior to 12.183-55; * 21.3 versions prior to 12.183-55; * 21.4 versions prior to 12.183-35; * 21.2 versions prior to 22.183-34 * 22.2 versions prior to 22.183-34 * 22.2 versions prior to 22.283-3 * 22.2 versions prior to 22.382-52, 22.383 * 22.2 versions prior to 22.482. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (12xpd) of Juniper Networks Junes OS and Junos OS Fovbed allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling its being done on the device. The impact of the Dzcpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVPP and LBPs. Alb, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS All versions prior to 20.483-58; * 21.1 versions prior to 21.383-54; * 21.2 versions prior to 21.383-54; * 21.4 versions prior to 21.483-33; * 22.1 versions prior to 22.482-53; * 22.2 versions prior to 22.482-53; * 22.3 versions prior to 22.483-53; * 22.4 versions prior to 22.483-53; * 22.5 versions prior to 22.483-53; * 22.5 versions prior to 22.483-53; * 22.6 versions prior to 22.483-53; * 22.7 versions prior to 22.483-53; * 22.8 versions prior to 22.483-53; * 22.9 versions prior to 22.4842-54; * 22.4 versions prior to 22.4842-54; * 22.5 versions prio						
* 21.1 versions prior to 21.183-54; * 21.2 versions prior to 21.283-52; * 21.3 versions prior to 13.813; * 21.4 versions prior to 22.181-52, 22.14R3; * 22.1 versions prior to 22.181-52, 22.14R3; * 22.1 versions prior to 22.181-52, 22.182. on PTX3000, PTX5000, QFX10000: * All versions prior to 20.483-58; * 21.1 version 21.181 and later versions; * 21.1 version 21.181 and later versions; * 21.2 versions prior to 12.183-55; * 21.3 versions prior to 12.183-55; * 21.4 versions prior to 12.183-35; * 21.2 versions prior to 22.183-34 * 22.2 versions prior to 22.183-34 * 22.2 versions prior to 22.283-3 * 22.2 versions prior to 22.382-52, 22.383 * 22.2 versions prior to 22.482. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (12xpd) of Juniper Networks Junes OS and Junos OS Fovbed allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling its being done on the device. The impact of the Dzcpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVPP and LBPs. Alb, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS All versions prior to 20.483-58; * 21.1 versions prior to 21.383-54; * 21.2 versions prior to 21.383-54; * 21.4 versions prior to 21.483-33; * 22.1 versions prior to 22.482-53; * 22.2 versions prior to 22.482-53; * 22.3 versions prior to 22.483-53; * 22.4 versions prior to 22.483-53; * 22.5 versions prior to 22.483-53; * 22.5 versions prior to 22.483-53; * 22.6 versions prior to 22.483-53; * 22.7 versions prior to 22.483-53; * 22.8 versions prior to 22.483-53; * 22.9 versions prior to 22.4842-54; * 22.4 versions prior to 22.4842-54; * 22.5 versions prio						
* 21.1 versions prior to 21.2R3-32; * 21.3 versions prior to 21.4R2-32, 21.4R3; * 21.4 versions prior to 21.4R2-32, 21.4R3; * 22.1 versions prior to 22.4R1-32, 22.4R2. on PTX3000, PTX5000, QFX100000: * All versions prior to 20.4R3-38; * 21.1 version 21.4R1 and later versions; * 21.1 versions prior to 21.2R3-36; * 21.3 versions prior to 21.2R3-36; * 21.4 versions prior to 21.4R3-34; * 22.4 versions prior to 21.4R3-34; * 22.1 versions prior to 22.4R3-34; * 22.2 versions prior to 22.4R3-34; * 22.2 versions prior to 22.2R3-31 * 22.2 versions prior to 22.2R3-31 * 22.2 versions prior to 22.2R3-31 * 22.3 versions prior to 22.2R3-32 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols deemon (l2xpp) of Analper Networks, lunss O5 and lunss O5 evolved allows so unauthensticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(In-05). This issue occurs when specific LLDP packets are received and telementy polling is being doen on the device. The impract of the 12cpd crash is reinitialization of STP protocols (ISTP, MSTP or VSTP), and MVRP and EBs. Alou, if any services depend on LLDP state (like PDE or VoIP) device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 version prior to 21.2R3-55; * 21.3 versions prior to 21.2R3-55; * 21.3 versions prior to 21.4R3-33; * 22.1 versions prior to 22.4R3-34; * 21.4 versions prior to 22.4R3-34; * 22.3 versions prior to 22.4R3-35; * 22.3 versions prior to 22.4R3-36; * 22.5 versions prior to 22.4R3-37; * 22.5 versions prior to 22.4R3-27; * 22.5 versions prior to 22.4R3-27; * 23.5 versions prior to 22.4R3-27; * 24.5 versions prior to 22.4R			•			
* 21.4 versions prior to 21.4R2-S2, 21.4R3; * 22.1 versions prior to 22.1R1-S2, 22.1R2. on PTX3000, PTX5000, QFX10000: * All versions prior to 20.4R3-S8; * 21.1 version prior to 21.8R3-S6; * 21.2 versions prior to 21.8R3-S6; * 21.3 versions prior to 21.8R3-S6; * 21.4 versions prior to 21.8R3-S6; * 21.4 versions prior to 21.8R3-S6; * 21.4 versions prior to 22.1R3-S3 * 22.2 versions prior to 22.1R3-S1 * 22.2 versions prior to 22.2R3-S1 * 22.2 versions prior to 22.3R2-S2, 22.3R3 * 22.4 versions prior to 22.3R2-S2, 22.3R3 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-Z control protocols deemon (12pq) of Juniper Networks Junes OS and Junes OS evolved allows an unauthenticated adjacent attacker who sends specific ILLDP packets to cause a Denial of Service(DoS). This issue occurs when specific ILLDP packets are received and telementry poling is being done on the device. The impact of the 12ppd crash is reinitialization of STP protocols (R3TP), MSTP or VSTP), and MVRP and REP. Also, if may services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version \$1.1R1 and later versions; * 21.2 versions prior to 21.7R3-S5; * 21.3 versions prior to 21.7R3-S5; * 21.3 versions prior to 21.7R3-S5; * 21.3 versions prior to 21.7R3-S5; * 21.4 versions prior to 21.7R3-S2; * 22.2 versions prior to 21.7R3-S2; * 22.3 versions prior to 22.7R3-S2; * 22.4 versions prior to 22.7R3-S2; * 22.2 versions prior to 22.7R3-S2; * 22.3 versions prior to 22.7R3-S2; * 22.3 versions prior to 22.7R3-S2; * 22.4 versions prior to 22.7R3-S2; * 22.5 versions prior to 22.7R3-S2; * 22.5 versions prior to 22.7R3-S2; * 22.5 versions prior to 22.7R3-S2; * 22.6 versions prior to 22.7R3-S2; * 22.7 versions prior to 22.7R3-S2;			· · · · · · · · · · · · · · · · · · ·			
* 22.1 versions prior to 22.1R1-52, 22.1R2. on PTX3000, PTX5000, QFX10000: * All versions prior to 20.4R3-58;			·			
on PTX3000, PTX5000, QFX10000: * All versions prior to 20.4R3-SR; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-SG; * 21.3 versions prior to 21.2R3-SG; * 21.4 versions prior to 21.2R3-SG; * 21.4 versions prior to 21.2R3-SG; * 21.4 versions prior to 21.2R3-SG; * 21.2 versions prior to 22.2R3-SG; * 22.2 versions prior to 22.2R3-SG; * 22.2 versions prior to 22.2R3-SG; * 22.3 versions prior to 22.2R3-SG; * 22.4 versions prior to 22.2R3-SG; * 22.4 versions prior to 22.4R3-SG; * 22.4 versions prior to 22.4R3-SG; * 22.5 versions prior to 22.4R3-SG; * 22.6 versions prior to 22.4R3-SG; * 22.7 versions prior to 22.4R3-SG; * 22.8 versions prior to 20.4R3-SG; * 23.1 version 21.1R1 and later versions; * 23.1 version 21.1R1 and later versions; * 23.2 versions prior to 21.2R3-SG; * 23.3 versions prior to 21.2R3-SG; * 23.1 versions prior to 21.2R3-SG; * 23.2 versions prior to 21.2R3-SG; * 23.2 versions prior to 21.2R3-SG; * 23.2 versions prior to 21.2R3-SG; * 23.3 versions prior to 21.2R3-SG; * 23.3 versions prior to 21.2R3-SG; * 24.2 versions prior to 21.2R3-SG; * 25.3 versions prior to 21.2R3-SG; * 26.2 versions prior to 21.2R3-SG; * 27.2 versions prior to 22.2R3-SG; * 27.2 versions p			·			
* All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.4R3-S4; * 22.1 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.4R3-S3 * 22.2 versions prior to 22.2R3-S1 * 22.3 versions prior to 22.2R3-S1 * 22.4 versions prior to 22.2R3-S1 * 22.4 versions prior to 22.2R3-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MWRP and RSP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 21.4R3-S3; * 21.1 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.4R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R3-S2; * 22.4 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R2-S2;			22.1 Versions prior to 22.11(1 52, 22.11(2.			
* All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.4R3-S4; * 22.1 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.4R3-S3 * 22.2 versions prior to 22.2R3-S1 * 22.3 versions prior to 22.2R3-S1 * 22.4 versions prior to 22.2R3-S1 * 22.4 versions prior to 22.2R3-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MWRP and RSP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 21.4R3-S3; * 21.1 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.4R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R3-S2; * 22.4 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R2-S2;						
* All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.4R3-S4; * 22.1 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.4R3-S3 * 22.2 versions prior to 22.2R3-S1 * 22.3 versions prior to 22.2R3-S1 * 22.4 versions prior to 22.2R3-S1 * 22.4 versions prior to 22.2R3-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.2R2-S2, 22.3R3 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MWRP and RSP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 21.4R3-S3; * 21.1 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.4R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R3-S2; * 22.4 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.2R2-S2;						
* 21.1 versions 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-56; * 21.3 versions prior to 21.8R3-56; * 21.4 versions prior to 21.4R3-56; * 21.2 versions prior to 21.4R3-56; * 22.1 versions prior to 22.1R3-53 * 22.2 versions prior to 22.2R3-51 * 22.3 versions prior to 22.2R3-51 * 22.4 versions prior to 22.2R3-51 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reintialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 versions prior to 21.1R3-55; * 21.3 versions prior to 21.4R3-53; * 21.4 versions prior to 21.4R3-53; * 21.2 versions prior to 21.4R3-53; * 22.1 versions prior to 22.2R3-5; * 22.2 versions prior to 22.2R3-5; * 22.3 versions prior to 22.2R3-5; * 22.4 versions prior to 22.2R3-5;			on PTX3000, PTX5000, QFX10000:			
* 21.1 versions 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-56; * 21.3 versions prior to 21.8R3-56; * 21.4 versions prior to 21.4R3-56; * 21.2 versions prior to 21.4R3-56; * 22.1 versions prior to 22.1R3-53 * 22.2 versions prior to 22.2R3-51 * 22.3 versions prior to 22.2R3-51 * 22.4 versions prior to 22.2R3-51 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reintialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 versions prior to 21.1R3-55; * 21.3 versions prior to 21.4R3-53; * 21.4 versions prior to 21.4R3-53; * 21.2 versions prior to 21.4R3-53; * 22.1 versions prior to 22.2R3-5; * 22.2 versions prior to 22.2R3-5; * 22.3 versions prior to 22.2R3-5; * 22.4 versions prior to 22.2R3-5;						
* 21.1 versions 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-56; * 21.3 versions prior to 21.8R3-56; * 21.4 versions prior to 21.4R3-56; * 21.2 versions prior to 21.4R3-56; * 22.1 versions prior to 22.1R3-53 * 22.2 versions prior to 22.2R3-51 * 22.3 versions prior to 22.2R3-51 * 22.4 versions prior to 22.2R3-51 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reintialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 versions prior to 21.1R3-55; * 21.3 versions prior to 21.4R3-53; * 21.4 versions prior to 21.4R3-53; * 21.2 versions prior to 21.4R3-53; * 22.1 versions prior to 22.2R3-5; * 22.2 versions prior to 22.2R3-5; * 22.3 versions prior to 22.2R3-5; * 22.4 versions prior to 22.2R3-5;						
* 21.2 versions prior to 21.283-56; * 21.3 versions prior to 21.383-55; * 21.4 versions prior to 21.483-54; * 22.1 versions prior to 22.183-53 * 22.2 versions prior to 22.283-51 * 22.3 versions prior to 22.382-52, 22.383 * 22.4 versions prior to 22.382-52, 22.383 * 22.4 versions prior to 22.482. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reintilialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PDE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 versions prior to 21.283-S5; * 21.3 versions prior to 21.483-S3; * 21.4 versions prior to 21.483-S3; * 22.1 versions prior to 21.483-S2; * 22.2 versions prior to 22.383-S2; * 22.2 versions prior to 22.383-S2; * 22.2 versions prior to 22.2872; * 22.3 versions prior to 22.3872-S2; * 22.4 versions prior to 22.3872-S2; * 22.4 versions prior to 22.482;			•			
* 21.3 versions prior to 21.3R3-55; * 21.4 versions prior to 22.4R3-54; * 22.2 versions prior to 22.2R3-51 * 22.3 versions prior to 22.2R3-51 * 22.3 versions prior to 22.2R3-51 * 22.4 versions prior to 22.2R3-53 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reintitalization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 versions prior to 21.1R3-S5; * 21.2 versions prior to 21.4R3-S3; * 21.2 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S2; * 22.2 versions prior to 22.2R3; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.4 versions prior to 22.2R3; * 22.4 versions prior to 22.2R5;			·			
* 22.1 versions prior to 22.183-53 * 22.2 versions prior to 22.283-51 * 22.3 versions prior to 22.282-52, 22.383 * 22.4 versions prior to 22.482. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS tvolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MYRP and ERP. Also, if any services depend on LLDP state (like POE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.483-58; * 21.1 version 21.181 and later versions; * 21.2 versions prior to 21.83-55; * 21.3 versions prior to 21.83-55; * 21.3 versions prior to 21.83-52; * 21.4 versions prior to 21.83-52; * 21.2 versions prior to 21.83-52; * 22.2 versions prior to 22.882; * 22.3 versions prior to 22.882; * 22.3 versions prior to 22.882; * 22.4 versions prior to 22.882; * 22.3 versions prior to 22.882;			,			
* 22.2 versions prior to 22.2R3-51 * 22.3 versions prior to 22.3R2-52, 22.3R3 * 22.4 versions prior to 22.3R2-52, 22.3R3 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-55; * 21.3 versions prior to 21.2R3-54; * 21.1 versions prior to 21.4R3-53; * 22.1 versions prior to 21.4R3-53; * 22.1 versions prior to 21.2R3-5; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.3 versions prior to 22.4R2; juniper - multiple * 22.4 versions prior to 22.4R2;			·			
* 22.3 versions prior to 22.3R2-S2, 22.3R3 * 22.4 versions prior to 22.4R2. An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DOS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.2R3; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.3 versions prior to 22.4R2; # 22.4 versions prior to 22.4R2;			·			
An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like Pot or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.3R3-S4; * 21.3 versions prior to 21.3R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R2-S2; * 22.4 versions prior to 22.4R2;						
in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.4R3-S3; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.4 versions prior to 22.3R3-S2; * 22.4 versions prior to 22.3R2-S2;			* 22.4 versions prior to 22.4R2.			
in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-55; * 21.3 versions prior to 21.2R3-55; * 21.4 versions prior to 21.4R3-53; * 22.1 versions prior to 22.1R3-52; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-52; * juniper - multiple * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52;						
in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-55; * 21.3 versions prior to 21.2R3-55; * 21.4 versions prior to 21.4R3-53; * 22.1 versions prior to 22.1R3-52; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-52; * juniper - multiple * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52;						
in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-55; * 21.3 versions prior to 21.2R3-55; * 21.4 versions prior to 21.4R3-53; * 22.1 versions prior to 22.1R3-52; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-52; * juniper - multiple * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52;						
in the Layer-2 control protocols daemon (I2cpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-58; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-55; * 21.3 versions prior to 21.2R3-55; * 21.4 versions prior to 21.4R3-53; * 22.1 versions prior to 22.1R3-52; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-52; * juniper - multiple * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52; * 22.4 versions prior to 22.3R2-52;						
Networks Junos OS and Junos OS Evolved allows an unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.2R3-S5; * 21.4 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.4 versions prior to 22.2R3; * 22.4 versions prior to 22.2R3; * 22.4 versions prior to 22.2R2; juniper - multiple * 22.4 versions prior to 22.4R2;						
unauthenticated adjacent attacker who sends specific LLDP packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.3R3-S4; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.1R3-S2; * 22.2 versions prior to 22.2R3; juniper - multiple variable All versions prior to 22.3R2-S2; * 22.4 versions prior to 22.3R2-S2; * 22.4 versions prior to 22.4R2;						
packets to cause a Denial of Service(DoS). This issue occurs when specific LLDP packets are received and telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.4R3-S2; * 22.2 versions prior to 22.4R3-S2; * 22.3 versions prior to 22.3R2-S2; juniper - multiple juniper - multiple						
telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;						
telemetry polling is being done on the device. The impact of the I2cpd crash is reinitialization of STP protocols (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S2; * 22.2 versions prior to 22.4R3-S2; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			This issue occurs when specific LLDP packets are received and			
VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.2 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.1R3-S2; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			· · · · · · · · · · · · · · · · · · ·			
state (like PoE or VoIP device recognition), then these will also be affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.2R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			· · · · · · · · · · · · · · · · · · ·			
affected. This issue affects: Juniper Networks Junos OS * All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 21.4 versions prior to 21.4R3-S2; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			. ,			
# All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;						
* All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			This issue affects:			
* All versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			Juniper Networks Junos OS			
* 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;						
* 21.1 version 21.1R1 and later versions; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;						
* 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			* All versions prior to 20.4R3-S8;			
* 21.3 versions prior to 21.3R3-S4; * 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			* 21.1 version 21.1R1 and later versions;			
* 21.4 versions prior to 21.4R3-S3; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			•			
* 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; juniper - multiple * 22.4 versions prior to 22.4R2;			· · · · · · · · · · · · · · · · · · ·			
* 22.3 versions prior to 22.3R2-S2; juniper - multiple			* 22.1 versions prior to 22.1R3-S2;			
juniper - multiple * 22.4 versions prior to 22.4R2;			·			
<u>CVE-2023-36839</u> products 2023-10-12 6.5 Medium		· · ·	· · · · · · · · · · · · · · · · · · ·			
	CVE-2023-36839	products		2023-10-12	6.5	Medium

Г					
		* All versions prior to 20.4R3-S8-EVO; * 21.1 version 21.1R1-EVO and later versions; * 21.2 versions prior to 21.2R3-S5-EVO; * 21.3 versions prior to 21.3R3-S4-EVO; * 21.4 versions prior to 21.4R3-S3-EVO; * 22.1 versions prior to 22.1R3-S2-EVO; * 22.2 versions prior to 22.2R3-EVO; * 22.3 versions prior to 22.3R2-S2-EVO; * 22.4 versions prior to 22.4R1-S1-EVO;			
		An Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in the management daemon (mgd) process of Juniper Networks Junos OS and Junos OS Evolved allows a network-based authenticated low-privileged attacker, by executing a specific command via NETCONF, to cause a CPU Denial of Service to the device's control plane. This issue affects: Juniper Networks Junos OS			
		* All versions prior to 20.4R3-S7; * 21.2 versions prior to 21.2R3-S5; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S1, 22.3R3; * 22.4 versions prior to 22.4R1-S2, 22.4R2.			
		# All versions prior to 21.4R3-S4-EVO; * 22.1 versions prior to 22.1R3-S2-EVO; * 22.2 versions prior to 22.2R3-EVO; * 22.3 versions prior to 22.3R3-EVO; * 22.4 versions prior to 22.4R2-EVO.			
		An indicator of compromise can be seen by first determining if the NETCONF client is logged in and fails to log out after a reasonable period of time and secondly reviewing the WCPU percentage for the mgd process by running the following command: mgd process example:			
		user@device-re#> show system processes extensive match "mgd PID" except last PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 92476 root 100 0 500M 89024K CPU3 3 57.5H 89.60% mgd <<<<<<< review the high cpu percentage. Example to check for NETCONF activity: While there is no specific command that shows a specific session in use for NETCONF, you can review logs for UI_LOG_EVENT with "client-mode 'netconf'"			
CVE-2023-44184	juniper - multiple products	For example:	2023-10-13	6.5	Medium

			1		1
		mgd[38121]: UI_LOGIN_EVENT: User 'root' login, class 'super-user' [38121], ssh-connection '10.1.1.1 201 55480 10.1.1.2 22', client-mode 'netconf'			
		An Improper Check for Unusual or Exceptional Conditions in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS Evolved on PTX10003 Series allows an unauthenticated adjacent attacker to cause an impact to the integrity of the system.			
		When specific transit MPLS packets are received by the PFE, these packets are internally forwarded to the RE. This issue is a prerequisite for CVE-2023-44195.			
		This issue affects Juniper Networks Junos OS Evolved:			
		* All versions prior to 20.4R3-S8-EVO; * 21.1-EVO version 21.1R1-EVO and later; * 21.2-EVO versions prior to 21.2R3-S6-EVO; * 21.3-EVO version 21.3R1-EVO and later; * 21.4-EVO versions prior to 21.4R3-S3-EVO; * 22.1-EVO versions prior to 22.1R3-S4-EVO; * 22.2-EVO versions prior to 22.2R3-S3-EVO; * 22.3-EVO versions prior to 22.3R2-S2-EVO, 22.3R3-EVO; * 22.4-EVO versions prior to 22.4R2-EVO.			
CVE-2023-44196	juniper - multiple products		2023-10-13	6.5	Medium
		An Improper Check or Handling of Exceptional Conditions vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on QFX5000 Series, EX2300, EX3400, EX4100, EX4400 and EX4600 allows a adjacent attacker to send specific traffic, which leads to packet flooding, resulting in a Denial of Service (DoS). When a specific IGMP packet is received in an isolated VLAN, it is duplicated to all other ports under the primary VLAN, which causes a flood. This issue affects QFX5000 series, EX2300, EX3400, EX4100, EX4400 and EX4600 platforms only.			
		This issue affects Juniper Junos OS on on QFX5000 Series, EX2300, EX3400, EX4100, EX4400 and EX4600:			
		* All 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-S5; * 21.4 versions prior to 21.4R3-S2; * 22.1 versions prior to 22.1R3; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2.			
CVE-2023-44203	juniper - multiple products		2023-10-13	6.5	Medium
		An Improper Validation of Syntactic Correctness of Input vulnerability in Routing Protocol Daemon (rpd) Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS).			
		When a malformed BGP UPDATE packet is received over an established BGP session, the rpd crashes and restarts.			
		This issue affects both eBGP and iBGP implementations.			
		This issue affects: Juniper Networks Junos OS			
CVE-2023-44204	juniper - multiple products	•	2023-10-13	6.5	Medium

	T				T 1
		 * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2-S1, 22.4R3; * 23.2 versions prior to 23.2R1, 23.2R2; 			
		Juniper Networks Junos OS Evolved			
		 * 21.4 versions prior to 21.4R3-S5-EVO; * 22.1 versions prior to 22.1R3-S3-EVO; * 22.2 versions prior to 22.2R3-S3-EVO; * 22.3 versions prior to 22.3R2-S2-EVO; * 22.4 versions prior to 22.4R3-EVO; * 23.2 versions prior to 23.2R2-EVO; 			
CVE-2023-42663	apache - airflow	Apache Airflow, versions before 2.7.2, has a vulnerability that allows an authorized user who has access to read specific DAGs only, to read information about task instances in other DAGs. Users of Apache Airflow are advised to upgrade to version 2.7.2 or newer to mitigate the risk associated with this vulnerability.	2023-10-14	6.5	Medium
		Apache Airflow, versions prior to 2.7.2, contains a security vulnerability that allows authenticated users of Airflow to list warnings for all DAGs, even if the user had no permission to see those DAGs. It would reveal the dag_ids and the stack-traces of import errors for those DAGs with import errors.			
CVE-2023-42780	apache - airflow	Users of Apache Airflow are advised to upgrade to version 2.7.2 or newer to mitigate the risk associated with this vulnerability.	2023-10-14	6.5	Medium
		Apache Airflow, in versions prior to 2.7.2, contains a security vulnerability that allows an authenticated user with limited access to some DAGs, to craft a request that could give the user write access to various DAG resources for DAGs that the user had no access to, thus, enabling the user to clear DAGs they shouldn't. Users of Apache Airflow are strongly advised to upgrade to version			
CVE-2023-42792	anache airfleui	2.7.2 or newer to mitigate the risk associated with this vulnerability.	2023-10-14	6.5	Medium
CVE-2025-42/92	apache - airflow	In tbd of tbd, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not	2025-10-14	0.5	Wedium
CVE-2023-35645	google - android	needed for exploitation. An issue was discovered in lib/kobject.c in the Linux kernel before	2023-10-11	6.4	Medium
CVE-2023-45863	linux - linux_kernel	6.2.3. With root access, an attacker can trigger a race condition that results in a fill_kobj_path out-of-bounds write. Use after free in Cast in Google Chrome prior to 118.0.5993.70	2023-10-14	6.4	Medium
CVE-2023-5473	google - chrome microsoft - multiple	allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low) Microsoft Dynamics 365 (on-premises) Cross-site Scripting	2023-10-11	6.3	Medium
CVE-2023-36416	products	Vulnerability	2023-10-10	6.1	Medium
CVE-2023-41680	fortinet - multiple products	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7 and 2.5.0 through 2.5.2 and 2.4.1 allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2023-10-13	6.1	Medium
CVE-2023-41681	fortinet - multiple products	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.7 and 2.5.0 through 2.5.2 and 2.4.1 allows attacker to execute unauthorized code or commands via crafted HTTP requests. An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.0 and 4.2.0 through 4.2.4, and 4.0.0 through 4.0.4 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.4 through 3.0.7 allows	2023-10-13	6.1	Medium
CVE-2023-41836	fortinet - multiple products	attacker to execute unauthorized code or commands via crafted HTTP requests.	2023-10-13	6.1	Medium

		A flaw was found in the Notfilter subsystem in the Linux kernel			
		A flaw was found in the Netfilter subsystem in the Linux kernel. The nfnl_osf_add_callback function did not validate the user mode			
		controlled opt_num field. This flaw allows a local privileged			
		(CAP_NET_ADMIN) attacker to trigger an out-of-bounds read,			
CVE-2023-39189	linux - linux_kernel	leading to a crash or information disclosure.	2023-10-09	6	Medium
		A flaw was found in the Netfilter subsystem in the Linux kernel.			
		The xt_u32 module did not validate the fields in the xt_u32 structure. This flaw allows a local privileged attacker to trigger an			
		out-of-bounds read by setting the size fields with a value beyond			
CVE-2023-39192	linux - linux_kernel	the array boundaries, leading to a crash or information disclosure.	2023-10-09	6	Medium
		A flaw was found in the Netfilter subsystem in the Linux kernel.			
		The sctp_mt_check did not validate the flag_count field. This flaw			
CVE 2022 20102	linux linux kornol	allows a local privileged (CAP_NET_ADMIN) attacker to trigger an	2023-10-09	6	Medium
CVE-2023-39193	linux - linux_kernel	out-of-bounds read, leading to a crash or information disclosure. IBM Security Directory Server 6.4.0 could allow a remote attacker	2023-10-09	0	Medium
		to obtain sensitive information, caused by the failure to properly			
		enable HTTP Strict Transport Security. An attacker could exploit			
	ibm - multiple	this vulnerability to obtain sensitive information using man in the			
CVE-2022-33161	products	middle techniques. X-Force ID: 228569.	2023-10-14	5.9	Medium
	google multiple	In phasecheckserver, there is a possible missing permission check.			
CVE-2023-40633	google - multiple products	This could lead to local information disclosure with no additional execution privileges needed	2023-10-08	5.5	Medium
CVL 2023 40033	products	In telecom service, there is a possible missing permission check.	2023 10 08	3.3	Wicalaili
	google - multiple	This could lead to local information disclosure with no additional			
CVE-2023-40637	products	execution privileges	2023-10-08	5.5	Medium
		In SoundRecorder service, there is a possible missing permission			
CVE 2022 40620	google android	check. This could lead to local information disclosure with no	2023-10-08	5.5	Medium
CVE-2023-40639	google - android	additional execution privileges In SoundRecorder service, there is a possible missing permission	2023-10-08	5.5	iviedium
		check. This could lead to local information disclosure with no			
CVE-2023-40640	google - android	additional execution privileges	2023-10-08	5.5	Medium
		In Messaging, there is a possible missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-40641	products	execution privileges needed	2023-10-08	5.5	Medium
	google - multiple	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional			
CVE-2023-40642	products	execution privileges needed	2023-10-08	5.5	Medium
	'	In Messaging, there is a possible missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-40643	products	execution privileges needed	2023-10-08	5.5	Medium
	google - multiple	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional			
CVE-2023-40644	products	execution privileges needed	2023-10-08	5.5	Medium
	'	In Messaging, there is a possible missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-40645	products	execution privileges needed	2023-10-08	5.5	Medium
CVE-2023-40645	·	In Messaging, there is a possible missing permission check. This	2023-10-08	5.5	Medium
	google - multiple	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional			
CVE-2023-40645 CVE-2023-40646	·	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-10-08	5.5	Medium Medium
	google - multiple	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional			
	google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed			
CVE-2023-40646	google - multiple products google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This	2023-10-08	5.5	Medium
CVE-2023-40646 CVE-2023-40647	google - multiple products google - multiple products google - multiple	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional	2023-10-08	5.5	Medium Medium
CVE-2023-40646	google - multiple products google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-10-08	5.5	Medium
CVE-2023-40646 CVE-2023-40647	google - multiple products google - multiple products google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional	2023-10-08	5.5	Medium Medium
CVE-2023-40646 CVE-2023-40647	google - multiple products google - multiple products google - multiple	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This	2023-10-08	5.5	Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648	google - multiple products google - multiple products google - multiple products google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check.	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649	google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648	google - multiple products google - multiple products google - multiple products google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check.	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649	google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649	google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649	google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649	google - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the	2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650	google - multiple products foogle - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650	google - multiple products foogle - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ	2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650	google - multiple products for multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note:	2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650 CVE-2023-41253	google - multiple products fo - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support	2023-10-08 2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650	google - multiple products for multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium
CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650 CVE-2023-41253	google - multiple products fo - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support	2023-10-08 2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium Medium
CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650 CVE-2023-41253	google - multiple products fo - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. An insertion of sensitive information into log file vulnerability in	2023-10-08 2023-10-08 2023-10-08 2023-10-08 2023-10-08	5.5 5.5 5.5 5.5	Medium Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40650 CVE-2023-41253 CVE-2023-43485 CVE-2023-25604	google - multiple products f5 - multiple products f5 - multiple products f5 - multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. An insertion of sensitive information into log file vulnerability in Fortinet FortiGuest 1.0.0 allows a local attacker to access plaintext passwords in the RADIUS logs.	2023-10-08 2023-10-08 2023-10-08 2023-10-08 2023-10-10 2023-10-10	5.5 5.5 5.5 5.5 5.5	Medium Medium Medium Medium Medium Medium Medium
CVE-2023-40646 CVE-2023-40647 CVE-2023-40648 CVE-2023-40649 CVE-2023-40650 CVE-2023-41253 CVE-2023-43485	google - multiple products for multiple products for multiple products	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. An insertion of sensitive information into log file vulnerability in Fortinet FortiGuest 1.0.0 allows a local attacker to access plaintext	2023-10-08 2023-10-08 2023-10-08 2023-10-08 2023-10-10	5.5 5.5 5.5 5.5 5.5	Medium Medium Medium Medium Medium Medium

	microsoft - multiple	Windows Power Management Service Information Disclosure			
CVE-2023-36724	products	Vulnerability	2023-10-10	5.5	Medium
CVE-2023-36728	microsoft - multiple products	Microsoft SQL Server Denial of Service Vulnerability	2023-10-10	5.5	Medium
<u>CVE-2023-30728</u>	products	Adobe Bridge versions 12.0.4 (and earlier) and 13.0.3 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	2023-10-10	5.5	iviedium
CVE-2023-38216	adobe - multiple products	vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-10-11	5.5	Medium
CVE-2023-38217	adobe - multiple products	Adobe Bridge versions 12.0.4 (and earlier) and 13.0.3 (and earlier) are affected by an Out-of-bounds Read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. An Exposure of Sensitive Information vulnerability in the 'file copy' command of Junos OS Evolved allows a local, authenticated attacker with shell access to view passwords supplied on the CLI command-line. These credentials can then be used to provide unauthorized access to the remote system.	2023-10-11	5.5	Medium
	juniper - multiple	This issue affects Juniper Networks Junos OS Evolved: * All versions prior to 20.4R3-S7-EVO; * 21.1 versions 21.1R1-EVO and later; * 21.2 versions prior to 21.2R3-S5-EVO; * 21.3 versions prior to 21.3R3-S4-EVO; * 21.4 versions prior to 21.4R3-S4-EVO; * 22.1 versions prior to 22.1R3-S2-EVO; * 22.2 versions prior to 22.2R2-EVO.			
CVE-2023-44187	products	SnapGathers versions prior to 4.9 are susceptible to a vulnerability	2023-10-11	5.5	Medium
		which could allow a local authenticated attacker to discover			
CVE-2023-27315	netapp - snapgathers	plaintext domain user credentials	2023-10-12	5.5	Medium
		A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos OS allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service. Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks: Junos OS: * All versions prior to 20.4R3-S8; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 22.1 versions prior to 22.1R3-S3; * 22.3 versions prior to 22.3R3; * 22.4 versions prior to 22.4R3.			
CVE-2023-44176	juniper - multiple products		2023-10-13	5.5	Medium
		A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos and Junos EVO allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service.			
		Repeated actions by the attacker will create a sustained Denial of Service (DoS) condition.			
		This issue affects Juniper Networks:			
		Junos OS:			
CVE-2023-44177	juniper - multiple products	* 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-S12; * 20.2 versions prior to 20.2R3-S8;	2023-10-13	5.5	Medium

		* 20.4 versions prior to 20.4R3-S8; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S3; * 23.2 versions prior to 23.2R3-S1;			
		 * 22.2 versions prior to 22.2R3-S1; * 22.3 versions prior to 22.3R3; * 22.4 versions prior to 22.4R2. 			
		Junos OS Evolved:			
		* All versions prior to 20.4R3-S8-EVO; * 21.2 versions prior to 21.2R3-S6-EVO; * 21.3 versions prior to 21.3R3-S5-EVO; * 21.4 versions prior to 21.4R3-S4-EVO; * 22.1 versions prior to 22.1R3-S3-EVO; * 22.2 versions prior to 22.2R3-S1-EVO; * 22.3 versions prior to 22.3R3-EVO; * 22.4 versions prior to 22.4R2-EVO.			
		A Stack-based Buffer Overflow vulnerability in the CLI command of Juniper Networks Junos OS allows a low privileged attacker to execute a specific CLI commands leading to Denial of Service. Repeated actions by the attacker will create a sustained Denial of			
		Service (DoS) condition.			
		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-S12; * 20.2 versions prior to 20.2R3-S8; * 20.4 versions prior to 20.4R3-S8; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R3-S1; * 22.4 versions prior to 22.4R2-S1; * 23.2 versions prior to 23.2R2.			
CVE-2023-44178	juniper - multiple products		2023-10-13	5.5	Medium
		An Improper Release of Memory Before Removing Last Reference vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a local, low privileged attacker to cause an FPC crash, leading to Denial of Service (DoS).			
		On all Junos MX Series with MPC1 - MPC9, LC480, LC2101, MX10003, and MX80, when Connectivity-Fault-Management (CFM) is enabled in a VPLS scenario, and a specific LDP related command is run, an FPC will crash and reboot. Continued execution of this specific LDP command can lead to sustained Denial of Service condition.			
		This issue affects:			
CVE-2023-44193	juniper - multiple products	Juniper Networks Junos OS on MX Series:	2023-10-13	5.5	Medium

		* All 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-S4; * 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.			
		An Incorrect Permission Assignment for Critical Resource vulnerability in a specific file of Juniper Networks Junos OS and Junos OS Evolved allows a local authenticated attacker to read configuration changes without having the permissions. When a user with the respective permissions commits a configuration change, a specific file is created. That file is readable even by users with no permissions to access the configuration. This can lead to privilege escalation as the user can read the password hash when a password change is being committed. This issue affects:			
		 * All versions prior to 20.4R3-S4; * 21.1 versions prior to 21.1R3-S4; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R2-S2, 21.3R3-S1; * 21.4 versions prior to 21.4R2-S1, 21.4R3. 			
		* All versions prior to 20.4R3-S4-EVO; * 21.1 versions prior to 21.1R3-S2-EVO; * 21.2 versions prior to 21.2R3-S2-EVO; * 21.3 versions prior to 21.3R3-S1-EVO; * 21.4 versions prior to 21.4R2-S2-EVO.			
CVE-2023-44201	juniper - multiple products	An integer overflow flaw was found in the Linux kernel. This issue leads to the kernel allocating `skb_shared_info` in the userspace,	2023-10-13	5.5	Medium
CVE-2023-42752	linux - linux_kernel ibm - multiple	which is exploitable in systems without SMAP protection since `skb_shared_info` contains references to function pointers. IBM App Connect Enterprise 11.0.0.1 through 11.0.0.23, 12.0.1.0 through 12.0.10.0 and IBM Integration Bus 10.1 through 10.1.0.1 are vulnerable to a denial of service for integration nodes on	2023-10-13	5.5	Medium
CVE-2023-45176 CVE-2023-42473	products sap - s\/4hana	Windows. IBM X-Force ID: 247998. S/4HANA Manage (Withholding Tax Items) - version 106, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges which has low impact on the confidentiality and integrity of the application.	2023-10-14	5.5 5.4	Medium Medium
CVE-2023-42474	sap - businessobjects_w eb_intelligence	SAP BusinessObjects Web Intelligence - version 420, has a URL with parameter that could be vulnerable to XSS attack. The attacker could send a malicious link to a user that would possibly allow an attacker to retrieve the sensitive information. A vulnerability has been identified in SINEC NMS (All versions < V2.0). The affected application improperly sanitizes certain SNMP	2023-10-10	5.4	Medium
CVE-2023-44315 CVE-2023-36555	siemens - sinec_nms fortinet - fortios	configuration data retrieved from monitored devices. An attacker with access to a monitored device could prepare a stored cross-site scripting (XSS) attack that may lead to unintentional modification of application data by legitimate users. An improper neutralization of script-related html tags in a web page (basic xss) in Fortinet FortiOS 7.2.0 - 7.2.4 allows an attacker	2023-10-10	5.4	Medium Medium

		to execute unauthorized code or commands via the SAML and Security Fabric components.			
		An improper neutralization of input during web page generation			
		vulnerability [CWE-79] in FortiMail version 7.2.0 through 7.2.2 and			
	fortinet - multiple	before 7.0.5 allows an authenticated attacker to inject HTML tags			
CVE-2023-36637	products	in FortiMail's calendar via input fields.	2023-10-10	5.4	Medium
CVE-2023-36584	microsoft - multiple products	Windows Mark of the Web Security Feature Bypass Vulnerability	2023-10-10	5.4	Medium
CVL-2023-30304	products	villuows wark of the web security reactive bypass vullerability	2023-10-10	<u> </u>	iviculum
		An Origin Validation vulnerability in MAC address validation of			
		Juniper Networks Junos OS Evolved on PTX10003 Series allows a			
		network-adjacent attacker to bypass MAC address checking,			
		allowing MAC addresses not intended to reach the adjacent LAN to be forwarded to the downstream network. Due to this issue, the			
		router will start forwarding traffic if a valid route is present in			
		forwarding-table, causing a loop and congestion in the			
		downstream layer-2 domain connected to the device.			
		This issue affects luninar Naturarks lungs OS Evalvad on PTV10003			
		This issue affects Juniper Networks Junos OS Evolved on PTX10003 Series:			
		Series.			
		* 411			
		* All versions prior to 21.4R3-S4-EVO;* 22.1 versions prior to 22.1R3-S3-EVO;			
		* 22.2 version 22.2R1-EVO and later versions;			
		* 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO;			
		* 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO;			
		* 23.2 versions prior to 23.2R2-EVO.			
	juniper - multiple				
CVE-2023-44189	products		2023-10-11	5.4	Medium
		An Origin Validation vulnerability in MAC address validation of			
		Juniper Networks Junos OS Evolved on PTX10001, PTX10004,			
		PTX10008, and PTX10016 devices allows a network-adjacent			
		attacker to bypass MAC address checking, allowing MAC addresses			
		not intended to reach the adjacent LAN to be forwarded to the			
		downstream network. Due to this issue, the router will start forwarding traffic if a valid route is present in forwarding-table,			
		causing a loop and congestion in the downstream layer-2 domain			
		connected to the device.			
		This is a self-stand of self-s			
		This issue affects Juniper Networks Junos OS Evolved on PTX10001, PTX10004, PTX10008, and PTX10016:			
		1 1X10001,1 1X10004,1 1X10000, and 1 1X10010.			
		* All versions prior to 21 AD2 CE EVO.			
		* All versions prior to 21.4R3-S5-EVO;* 22.1 versions prior to 22.1R3-S4-EVO;			
		* 22.2 versions 22.2R1-EVO and later;			
		* 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO;			
		* 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO;			
		* 23.2 versions prior to 23.2R1-S1-EVO, 23.2R2-EVO.			
	i			i	
				ļ	
CVF-2023-44190	juniper - multiple		2023-10-11	5 4	Medium
CVE-2023-44190	juniper - multiple products zabbix - multiple	A stored XSS has been found in the Zabbix web application in the	2023-10-11	5.4	Medium
CVE-2023-44190 CVE-2023-32721	products	Maps element if a URL field is set with spaces before URL.	2023-10-11 2023-10-12	5.4 5.4	Medium Medium
	products zabbix - multiple	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability			
	products zabbix - multiple products	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from			
CVE-2023-32721	products zabbix - multiple products wordpress -	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7	2023-10-12	5.4	Medium
	products zabbix - multiple products	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from			
CVE-2023-32721	products zabbix - multiple products wordpress -	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and	2023-10-12	5.4	Medium
CVE-2023-32721	products zabbix - multiple products wordpress - multiple products	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows	2023-10-12	5.4	Medium
CVE-2023-32721 CVE-2023-38000	products zabbix - multiple products wordpress - multiple products fortinet - multiple	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows attacker to execute unauthorized code or commands via crafted	2023-10-12	5.4	Medium Medium
CVE-2023-32721	products zabbix - multiple products wordpress - multiple products	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows	2023-10-12	5.4	Medium
CVE-2023-32721 CVE-2023-38000	products zabbix - multiple products wordpress - multiple products fortinet - multiple	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2023-10-12	5.4	Medium
CVE-2023-32721 CVE-2023-38000	products zabbix - multiple products wordpress - multiple products fortinet - multiple	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows attacker to execute unauthorized code or commands via crafted HTTP requests. A cross-site scripting (XSS) vulnerability has been reported to	2023-10-12	5.4	Medium Medium
CVE-2023-32721 CVE-2023-38000	products zabbix - multiple products wordpress - multiple products fortinet - multiple products	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows attacker to execute unauthorized code or commands via crafted HTTP requests. A cross-site scripting (XSS) vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network.	2023-10-12	5.4	Medium
CVE-2023-32721 CVE-2023-38000 CVE-2023-41843	products zabbix - multiple products wordpress - multiple products fortinet - multiple products qnap -	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows attacker to execute unauthorized code or commands via crafted HTTP requests. A cross-site scripting (XSS) vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version:	2023-10-12 2023-10-13 2023-10-13	5.4	Medium Medium Medium
CVE-2023-32721 CVE-2023-38000	products zabbix - multiple products wordpress - multiple products fortinet - multiple products	Maps element if a URL field is set with spaces before URL. Auth. Stored (contributor+) Cross-Site Scripting (XSS) vulnerability in WordPress core 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.1.3, from 6.0 through 6.0.5, from 5.9 through 5.9.7 and Gutenberg plugin <= 16.8.0 versions. A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 allows attacker to execute unauthorized code or commands via crafted HTTP requests. A cross-site scripting (XSS) vulnerability has been reported to affect Video Station. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network.	2023-10-12	5.4	Medium Medium

		Web III thus altering the intended functionality potentially leading	<u> </u>		1
		Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 263376.			
		A use after free vulnerability [CWE-416] in FortiOS version 7.2.0 through 7.2.4 and version 7.0.0 through 7.0.10 and FortiProxy version 7.2.0 through 7.2.2 and version 7.0.0 through 7.0.8 may			
	fortinet - multiple	allow an unauthenticated remote attacker to crash the WAD process via multiple crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet			
CVE-2023-41675	products	inspection. A insufficient verification of data authenticity vulnerability [CWE-	2023-10-10	5.3	Medium
	fortinet - multiple	345] in FortiAnalyzer version 7.4.0 and below 7.2.3 allows a remote unauthenticated attacker to send messages to the syslog server of FortiAnalyzer via the knoweldge of an authorized device			
CVE-2023-42782	products microsoft - multiple	serial number.	2023-10-10	5.3	Medium
CVE-2023-41763	products	Skype for Business Elevation of Privilege Vulnerability Incomplete Cleanup vulnerability in Apache Tomcat.When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an error could cause Tomcat to skip some parts of the recycling process leading to	2023-10-10	5.3	Medium
	apache - multiple	information leaking from the current request/response to the next. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards,			
<u>CVE-2023-42795</u>	products	which fixes the issue. Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.	2023-10-10	5.3	Medium
CVE-2023-45648	apache - multiple products	Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.	2023-10-10	5.3	Medium
CVE-2023-44094	huawei - multiple products	Type confusion vulnerability in the distributed file module. Successful exploitation of this vulnerability may cause the device to restart.	2023-10-11	5.3	Medium
	huawei - multiple	Parameter verification vulnerability in the window module.Successful exploitation of this vulnerability may cause the			
CVE-2023-41304	products	size of an app window to be adjusted to that of a floating window. Broadcast permission control vulnerability in the Bluetooth	2023-10-11	5.3	Mediun
CVE-2023-44102	huawei - multiple products	module.Successful exploitation of this vulnerability can cause the Bluetooth function to be unavailable.	2023-10-11	5.3	Mediun
		A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in telemetry processing of Juniper Networks Junos OS allows a network-based authenticated attacker to flood the system with multiple telemetry requests, causing the Junos Kernel Debugging Streaming Daemon (jkdsd) process to crash, leading to a Denial of Service (DoS). Continued receipt and processing of telemetry requests will repeatedly crash the jkdsd process and sustain the Denial of Service (DoS) condition.			
		This issue is seen on all Junos platforms. The crash is triggered when multiple telemetry requests come from different collectors. As the load increases, the Dynamic Rendering Daemon (drend) decides to defer processing and continue later, which results in a timing issue accessing stale memory, causing the jkdsd process to crash and restart.			
		This issue affects:			
		Juniper Networks Junos OS:			
CVE-2023-44188	juniper - multiple products	 * 20.4 versions prior to 20.4R3-S9; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; 	2023-10-11	5.3	Medium

	T		T		, ,
		 * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S1, 22.3R3-S1; * 22.4 versions prior to 22.4R2-S2, 22.4R3; * 23.1 versions prior to 23.1R2; * 23.2 versions prior to 23.2R2. 			
		This issue does not affect Juniper Networks Junos OS versions prior to 19.4R1.			
		An Improper Input Validation vulnerability in the VxLAN packet forwarding engine (PFE) of Juniper Networks Junos OS on QFX5000 Series, EX4600 Series devices allows an unauthenticated, adjacent attacker, sending two or more genuine packets in the same VxLAN topology to possibly cause a DMA memory leak to occur under various specific operational conditions. The scenario described here is the worst-case scenario. There are other scenarios that require operator action to occur.			
		An indicator of compromise may be seen when multiple devices indicate that FPCO has gone missing when issuing a show chassis fpc command for about 10 to 20 minutes, and a number of interfaces have also gone missing.			
		Use the following command to determine if FPCO has gone missing from the device.			
		show chassis fpc detail This issue affects:			
		Juniper Networks Junos OS on QFX5000 Series, EX4600 Series:			
		 * 18.4 version 18.4R2 and later versions prior to 20.4R3-S8; * 21.1 version 21.1R1 and later versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S1; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2. 			
CVE-2023-44183	juniper - multiple products		2023-10-13	5.3	Medium
CVE-2023-38251	adobe - multiple products	Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by a Uncontrolled Resource Consumption vulnerability that could lead in minor application denial-of-service. Exploitation of this issue does not require user interaction.	2023-10-13	5.3	Medium
CVE-2022-43868	ibm - security_verify_acc ess_oidc_provider	IBM Security Verify Access OIDC Provider could disclose directory information that could aid attackers in further attacks against the system. IBM X-Force ID: 239445.	2023-10-14	5.3	Medium
CVE-2022-43868 CVE-2023-26367	adobe - multiple products	Adobe Commerce versions 2.4.7-beta1 (and earlier), 2.4.6-p2 (and earlier), 2.4.5-p4 (and earlier) and 2.4.4-p5 (and earlier) are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction. A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to launch a denial-of-service (DoS) attack via a network. QES is not affected.	2023-10-14	4.9	Medium
CVE-2023-32970	qnap - multiple products	We have already fixed the vulnerability in the following versions: QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.0.2453 build 20230708 and later QuTS hero h4.5.4.2476 build 20230728 and later QuTScloud c5.1.0.2498 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later	2023-10-13	4.9	Medium

		In Dialor, there is a possible missing permission shock. This sould			1
	google - multiple	In Dialer, there is a possible missing permission check. This could lead to local information disclosure with System execution			
CVE-2023-40631	products	privileges needed	2023-10-08	4.4	Medium
		In telecom service, there is a possible way to write permission			
		usage records of an app due to a missing permission check. This could lead to local information disclosure with System execution			
CVE-2023-40636	google - android	privileges needed	2023-10-08	4.4	Medium
		In Telecom service, there is a possible missing permission check.			
CVE-2023-40638	google android	This could lead to local denial of service with System execution	2023-10-08	4.4	Medium
CVE-2023-40638	google - android	In urild service, there is a possible out of bounds write due to a	2023-10-08	4.4	iviedium
	google - multiple	missing bounds check. This could lead to local denial of service			
CVE-2023-40651	products	with System execution privileges needed	2023-10-08	4.4	Medium
		In jpg driver, there is a possible out of bounds write due to			
CVE-2023-40652	google - android	improper input validation. This could lead to local denial of service with System execution privileges needed	2023-10-08	4.4	Medium
	google america	A flaw was found in the XFRM subsystem in the Linux kernel. The			
		specific flaw exists within the processing of state filters, which can			
	linux - multiple	result in a read past the end of an allocated buffer. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-			
CVE-2023-39194	products	bounds read, potentially leading to an information disclosure.	2023-10-09	4.4	Medium
	F - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	A vulnerability has been identified in SIMATIC CP 1604 (All			
		versions), SIMATIC CP 1616 (All versions), SIMATIC CP 1623 (All			
		versions), SIMATIC CP 1626 (All versions), SIMATIC CP 1628 (All versions). Affected devices insufficiently control continuous			
		mapping of direct memory access (DMA) requests. This could			
	siemens -	allow local attackers with administrative privileges to cause a			
0.45 2022 27405	simatic_cp_1604_fi	denial of service situation on the host. A physical power cycle is	2022 40 40		Na di di
CVE-2023-37195	rmware	required to get the system working again. A vulnerability has been identified in SICAM PAS/PQS (All versions	2023-10-10	4.4	Medium
		>= V8.00 < V8.22). The affected application is installed with			
		specific files and folders with insecure permissions. This could			
CVE-2023-38640	siemens - sicam_pas√pqs	allow an authenticated local attacker to read and modify configuration data in the context of the application process.	2023-10-10	4.4	Medium
CVE-2023-38040	sicam_pas (/ pqs	configuration data in the context of the application process.	2023-10-10	4.4	Medium
		When BIG-IP APM Guided Configurations are configured,			
		undisclosed sensitive information may be logged in restnoded			
		log.			
		Note: Software versions which have reached End of Technical			
		Support (EoTS) are not evaluated.			
CVE 2022 20447	f5 - multiple		2022 40 40	4.4	NA salinna
CVE-2023-39447	products		2023-10-10	4.4	Medium
		Exposure of Sensitive Information vulnerability exist in an			
		undisclosed BIG-IP TMOS shell (tmsh) command which may allow			
		an authenticated attacker with resource administrator role privileges to view sensitive information.			
		privileges to view sensitive information.			
		Note: Software versions which have reached End of Technical			
	والمناخات الم	Support (EoTS) are not evaluated.			
CVE-2023-45219	f5 - multiple products		2023-10-10	4.4	Medium
	microsoft - multiple				
CVE-2023-36698	products	Windows Kernel Security Feature Bypass Vulnerability	2023-10-10	4.4	Medium
CVE-2023-36722	microsoft - multiple products	Active Directory Domain Services Information Disclosure Vulnerability	2023-10-10	4.4	Medium
CVL-2023-30/22	products	In TBD of TBD, there is a possible way to access location	Z0Z2-10-10	4.4	ivicululli
		information due to a permissions bypass. This could lead to local			
0) (5,000,000,000,000		information disclosure with System execution privileges needed.	0000 15 11		
CVE-2023-35653	google - android	User interaction is not needed for exploitation. IBM App Connect Enterprise 12.0.1.0 through 12.0.8.0 contains an	2023-10-11	4.4	Medium
	ibm -	unspecified vulnerability that could allow a local privileged user to			
	app_connect_enter	obtain sensitive information from API logs. IBM X-Force ID:			
CVE-2023-40682	prise	263833.	2023-10-13	4.4	Medium
		SAP Business One (B1i) - version 10.0, allows an authorized attacker to retrieve the details stack trace of the fault message to			
		conduct the XXE injection, which will lead to information			
		disclosure. After successful exploitation, an attacker can cause			
	-	limited impact on the confidentiality and no impact to the integrity			
CVE 2022 442CE	can husingss	, , ,	2022 40 40	12	\
CVE-2023-41365	sap - business_one	and availability.	2023-10-10	4.3	Medium
CVE-2023-41365	sap - business_one sap - multiple	, , ,	2023-10-10	4.3	Medium
CVE-2023-41365 CVE-2023-42475		and availability. The Statutory Reporting application has a vulnerable file storage location, potentially enabling low privileged attacker to read server files with minimal impact on confidentiality.	2023-10-10	4.3	Medium Medium
	sap - multiple products	and availability. The Statutory Reporting application has a vulnerable file storage location, potentially enabling low privileged attacker to read server files with minimal impact on confidentiality. An improper access control vulnerability in Fortinet FortiOS 7.2.0 -			
	sap - multiple products fortinet - multiple	and availability. The Statutory Reporting application has a vulnerable file storage location, potentially enabling low privileged attacker to read server files with minimal impact on confidentiality.	2023-10-10	4.3	Medium
CVE-2023-42475	sap - multiple products	and availability. The Statutory Reporting application has a vulnerable file storage location, potentially enabling low privileged attacker to read server files with minimal impact on confidentiality. An improper access control vulnerability in Fortinet FortiOS 7.2.0 - 7.2.4 and 7.4.0 allows an attacker to access a restricted resource			

	T			1	1
		Inappropriate implementation in Installer in Google Chrome prior			
		to 118.0.5993.70 allowed a local attacker to bypass discretionary			
		access control via a crafted command. (Chromium security			
CVE-2023-5477	google - chrome	severity: Low)	2023-10-11	4.3	Medium
		Inappropriate implementation in Autofill in Google Chrome prior			
		to 118.0.5993.70 allowed a remote attacker to leak cross-origin			
CVE-2023-5478	google - chrome	data via a crafted HTML page. (Chromium security severity: Low)	2023-10-11	4.3	Medium
		Inappropriate implementation in Autofill in Google Chrome prior			
		to 118.0.5993.70 allowed a remote attacker to bypass autofill			
		restrictions via a crafted HTML page. (Chromium security severity:			
CVE-2023-5485	google - chrome	Low)	2023-10-11	4.3	Medium
	8008.0 00	Inappropriate implementation in Input in Google Chrome prior to			
		118.0.5993.70 allowed a remote attacker to spoof security UI via a			
CVE-2023-5486	google - chrome	crafted HTML page. (Chromium security severity: Low)	2023-10-11	4.3	Medium
CVE-2023-3460	google - chrome		2023-10-11	4.3	Medium
		SnapCenter Plugin for VMware vSphere versions 4.6 prior to 4.9			
		are			
		susceptible to a vulnerability which may allow authenticated			
		unprivileged users to modify email and snapshot name settings			
		within the			
	netapp -	VMware vSphere user interface.			
CVE-2023-27312	snapcenter_plug-in		2023-10-12	4.3	Medium
		Exposure of Sensitive Information to an Unauthorized Actor in			
		WordPress from 6.3 through 6.3.1, from 6.2 through 6.2.2, from			
		6.1 through 6.13, from 6.0 through 6.0.5, from 5.9 through 5.9.7,			
		from 5.8 through 5.8.7, from 5.7 through 5.7.9, from 5.6 through			
		5.6.11, from 5.5 through 5.5.12, from 5.4 through 5.4.13, from 5.3			
		through 5.3.15, from 5.2 through 5.2.18, from 5.1 through 5.1.16,			
		from 5.0 through 5.0.19, from 4.9 through 4.9.23, from 4.8			
		through 4.8.22, from 4.7 through 4.7.26, from 4.6 through 4.6.26,			
	wordpress -	from 4.5 through 4.5.29, from 4.4 through 4.4.30, from 4.3			
CVE-2023-39999	multiple products	through 4.3.31, from 4.2 through 4.2.35, from 4.1 through 4.1.38.	2023-10-13	4.3	Medium
<u>CVL 2023 33333</u>	manipic products	tillough 4.3.31, 110111 4.2 tillough 4.2.33, 110111 4.1 tillough 4.1.30.	2023 10 13	7.5	Wicalaiii
		Apache Airflow, versions 2.7.0 and 2.7.1, is affected by a			
		vulnerability that allows an authenticated user to retrieve sensitive			
		configuration information when the "expose_config" option is set			
		to "non-sensitive-only". The `expose_config` option is False by			
CVE 2022 45246	analis of G	default.	2022 40 44	4.0	N 4 = -1*
CVE-2023-45348	apache - airflow	It is recommended to upgrade to a version that is not affected.	2023-10-14	4.3	Medium
01/5 2022 2255	microsoft -		2022 12 12		
CVE-2023-36559	edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2023-10-13	4.2	Medium
		An exposure of sensitive information to an unauthorized actor			
		vulnerability [CWE-200] in FortiClient for Windows 7.2.0, 7.0 all			
		versions, 6.4 all versions, 6.2 all versions, Linux 7.2.0, 7.0 all			
		versions, 6.4 all versions, 6.2 all versions and Mac 7.2.0 through			
		7.2.1, 7.0 all versions, 6.4 all versions, 6.2 all versions, may allow a			
	fortinet - multiple	local authenticated attacker with no Administrative privileges to			
CVE-2023-37939	products	retrieve the list of files or folders excluded from malware scanning.	2023-10-10	3.3	Low
	hp -	A potential security vulnerability has been identified in certain HP			
	e22_g4_fhd_firmw	Displays supporting the Theft Deterrence feature which may allow			
CVE-2023-5449	are	a monitor's Theft Deterrence to be deactivated.	2023-10-13	3.3	Low

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's وإذ تبقى NIST's وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة. NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

متاح