تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 8 اكتوبر إلى 14 اكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
- عالي: النتيجة الأساسية لـCVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـCVSS 4.0-6.9
- منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 8th of October to 14th of October. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-41373	f5 - multiple products	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. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	9.9	Critical
CVE-2023-5365	hp - life	HP LIFE Android Mobile application is potentially vulnerable to escalation of privilege and/or information disclosure.	2023-10-09	9.8	Critical
CVE-2023-43625	siemens - simcenter_amesim	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 the affected application process.	2023-10-10	9.8	Critical
CVE-2023-34992	fortinet - multiple products	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 through 6.5.1 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via crafted API requests.	2023-10-10	9.8	Critical
CVE-2023-34993	fortinet - multiple 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 http get request parameters.	2023-10-10	9.8	Critical
CVE-2023-36547	fortinet - multiple 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 http get request parameters.	2023-10-10	9.8	Critical
CVE-2023-36548	fortinet - multiple 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 http get request parameters.	2023-10-10	9.8	Critical
CVE-2023-36549	fortinet - multiple 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 http get request parameters.	2023-10-10	9.8	Critical
CVE-2023-36550	fortinet - multiple 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 http get request parameters.	2023-10-10	9.8	Critical
CVE-2023-35349	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	9.8	Critical

CVE-2023-36419	microsoft - azure_hdinsights	Azure HDInsight Apache Oozie Workflow Scheduler Elevation of Privilege Vulnerability	2023-10-10	9.8	Critical
CVE-2023-36434	microsoft - multiple products	Windows IIS Server Elevation of Privilege Vulnerability	2023-10-10	9.8	Critical
CVE-2023-44106	huawei - multiple products	API permission management vulnerability in the Fwk-Display module.Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-10-11	9.8	Critical
CVE-2023-44105	huawei - multiple products	Vulnerability of permissions not being strictly verified in the window management module.Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-10-11	9.8	Critical
CVE-2023-44116	huawei - multiple products	Vulnerability of access permissions not being strictly verified in the APPWidget module.Successful exploitation of this vulnerability may cause some apps to run without being authorized.	2023-10-11	9.8	Critical
CVE-2023-35646	google - android	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 not needed for exploitation.	2023-10-11	9.8	Critical
CVE-2023-35647	google - android	In ProtocolEmbmsGlobalCellIdAdapter::Init() of protocolembmsadapter.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 required. User interaction is not needed for exploitation.	2023-10-11	9.8	Critical
CVE-2023-35648	google - android	In ProtocolMiscLceIndAdapter::GetConfLevel() of 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 required. User interaction is not needed for exploitation.	2023-10-11	9.8	Critical
CVE-2023-35662	google - android	there is a possible out of bounds write due to buffer overflow. This 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
CVE-2023-41679	fortinet - multiple products	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 "device management" permission on his profile and belonging to a specific ADOM to add and delete CLI script on other ADOMs	2023-10-10	9.6	Critical
CVE-2023-44981	apache - multiple products	Authorization Bypass Through User-Controlled Key vulnerability in 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 ensure the ensemble election/quorum communication is protected by a firewall as this will mitigate the issue. See the documentation for more details on correct cluster administration.	2023-10-11	9.1	Critical
CVE-2023-44107	huawei - harmonyos	Vulnerability of defects introduced in the design process in the screen projection module.Successful exploitation of this vulnerability may affect service availability and integrity.	2023-10-11	9.1	Critical
CVE-2023-44118	huawei - multiple products	Vulnerability of undefined permissions in the MeeTime module.Successful exploitation of this vulnerability will affect 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
CVE-2022-32755	ibm - multiple products	IBM Security Directory Server 6.4.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 228505.	2023-10-14	9.1	Critical
CVE-2023-42796	siemens - cp-8050_firmware	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. This could allow an authenticated remote attacker to traverse directories on the system and download arbitrary files. By	2023-10-10	8.8	High

متاح

		exploring active session IDs, the vulnerability could potentially be leveraged to escalate privileges to the administrator role.			
CVE-2023-34985	fortinet - multiple 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 HTTP get request parameters.	2023-10-10	8.8	High
CVE-2023-34986	fortinet - multiple 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 HTTP get request parameters.	2023-10-10	8.8	High
CVE-2023-34987	fortinet - multiple 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 HTTP get request parameters.	2023-10-10	8.8	High
CVE-2023-34988	fortinet - multiple 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 HTTP get request parameters.	2023-10-10	8.8	High
CVE-2023-34989	fortinet - multiple 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 HTTP get request parameters.	2023-10-10	8.8	High
CVE-2023-36556	fortinet - multiple products	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 and below 6.4.7 allows an authenticated attacker to login on other users accounts from the same web domain via crafted HTTP or HTTPs requests.	2023-10-10	8.8	High
CVE-2023-41841	fortinet - multiple products	An improper authorization vulnerability in Fortinet FortiOS 7.0.0 - 7.0.11 and 7.2.0 - 7.2.4 allows an attacker belonging to the prof-admin profile to perform elevated actions.	2023-10-10	8.8	High
CVE-2023-36414	microsoft - azure_identity_sdk	Azure Identity SDK Remote Code Execution Vulnerability	2023-10-10	8.8	High
CVE-2023-36415	microsoft - multiple products	Azure Identity SDK Remote Code Execution Vulnerability	2023-10-10	8.8	High
CVE-2023-36577	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2023-10-10	8.8	High
CVE-2023-37536	apache - multiple products	An integer overflow in xerces-c++ 3.2.3 in BigFix Platform allows remote attackers to cause out-of-bound access via HTTP request.	2023-10-11	8.8	High
CVE-2023-5218	google - chrome	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 severity: Critical)	2023-10-11	8.8	High
CVE-2023-5474	google - chrome	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: Medium)	2023-10-11	8.8	High
CVE-2023-5476	google - chrome	Use after free in Blink History 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 severity: Medium)	2023-10-11	8.8	High
CVE-2023-32724	zabbix - multiple products	Memory pointer is in a property of the Ducktape object. This leads to multiple vulnerabilities related to direct memory access and manipulation.	2023-10-12	8.8	High
CVE-2023-27313	netapp - snapcenter	SnapCenter versions 3.x and 4.x prior to 4.9 are susceptible to a vulnerability which may allow an authenticated unprivileged user to gain access as an admin user.	2023-10-12	8.8	High
CVE-2023-44182	juniper - multiple products	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. This issue affects:	2023-10-13	8.8	High

		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
CVE-2023-34975	qnap - video_station	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. 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-2023-34976	qnap - video_station	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. 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.	2023-10-10	8.7	High
CVE-2023-38219	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 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 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
CVE-2023-40537	f5 - multiple products	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 Support (EoTS) are not evaluated.	2023-10-10	8.1	High
CVE-2023-38166	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41765	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High

CVE-2023-41767	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41768	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41769	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41770	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41771	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41773	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-41774	microsoft - multiple products	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	2023-10-10	8.1	High
CVE-2023-33303	fortinet - fortiedr	A insufficient session expiration in Fortinet FortiEDR version 5.0.0 through 5.0.1 allows attacker to execute unauthorized code or commands via api request	2023-10-13	8.1	High
CVE-2023-36697	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	8	High
CVE-2023-36778	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-10-10	8	High
CVE-2023-40634	google - multiple products	In phasechecksercer, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-10-08	7.8	High
CVE-2023-40635	google - android	In linkturbo, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	2023-10-08	7.8	High
CVE-2022-3431	lenovo - ideapad_creator_5-16ach6_firmware	A potential vulnerability in a driver used during manufacturing process on some consumer Lenovo Notebook devices that was mistakenly not deactivated may allow an attacker with elevated privileges to modify secure boot setting by modifying an NVRAM variable.	2023-10-09	7.8	High
CVE-2022-30527	siemens - sinec_nms	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. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	2023-10-10	7.8	High
CVE-2023-30900	siemens - xpedition_layout_browser	A vulnerability has been identified in Xpedition Layout Browser (All versions < VX.2.14). Affected application contains a stack overflow vulnerability when parsing a PCB file. An attacker can leverage this vulnerability to execute code in the context of the current process.	2023-10-10	7.8	High
CVE-2023-36380	siemens - cp-8050_firmware	A vulnerability has been identified in CP-8031 MASTER MODULE (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 login to the device via SSH. Only devices with activated debug support are affected.	2023-10-10	7.8	High
CVE-2023-44081	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation 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 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
CVE-2023-44082	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation 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 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
CVE-2023-44083	siemens - multiple products	A vulnerability has been identified in Tecnomatix Plant Simulation 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 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
CVE-2023-44084	siemens - multiple products	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 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	High
CVE-2023-44085	siemens - multiple products	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	2023-10-10	7.8	High

متاح

		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.			
CVE-2023-44086	siemens - multiple products	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 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	High
CVE-2023-44087	siemens - multiple products	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 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	High
CVE-2023-45204	siemens - multiple products	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 a type confusion vulnerability while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21268)	2023-10-10	7.8	High
CVE-2023-45205	siemens - sicam_pas\/pqs	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 allow an authenticated local attacker to inject arbitrary code and escalate privileges to `NT AUTHORITY/SYSTEM`.	2023-10-10	7.8	High
CVE-2023-45601	siemens - multiple products	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 crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21290)	2023-10-10	7.8	High
CVE-2023-43611	f5 - multiple products	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-2023-38418. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2023-10-10	7.8	High
CVE-2023-5450	f5 - multiple products	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.	2023-10-10	7.8	High
CVE-2022-22298	fortinet - multiple products	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiIsolator version 1.0.0, FortiIsolator version 1.1.0, FortiIsolator version 1.2.0 through 1.2.2, FortiIsolator version 2.0.0 through 2.0.1, FortiIsolator version 2.1.0 through 2.1.2, FortiIsolator version 2.2.0, FortiIsolator 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
CVE-2023-25607	fortinet - multiple products	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-2023-42788	fortinet - multiple products	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 arguments to a CLI command	2023-10-10	7.8	High
CVE-2023-36417	microsoft - multiple products	Microsoft SQL OLE DB Remote Code Execution Vulnerability	2023-10-10	7.8	High

CVE-2023-36418	microsoft - azure_rtos_guix_studio	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36420	microsoft - multiple products	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36436	microsoft - multiple products	Windows MSHTML Platform Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36557	microsoft - multiple products	PrintHTML API Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36594	microsoft - multiple products	Windows Graphics Component Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36598	microsoft - multiple products	Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36605	microsoft - multiple products	Windows Named Pipe Filesystem Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36701	microsoft - multiple products	Microsoft Resilient File System (ReFS) Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36702	microsoft - multiple 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
CVE-2023-36710	microsoft - multiple products	Windows Media Foundation Core Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36711	microsoft - multiple products	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36712	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36718	microsoft - multiple products	Microsoft Virtual Trusted Platform Module Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36723	microsoft - multiple products	Windows Container Manager Service Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36725	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36726	microsoft - multiple products	Windows Internet Key Exchange (IKE) Extension Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36729	microsoft - multiple products	Named Pipe File System Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36730	microsoft - multiple products	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36731	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36732	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36737	microsoft - azure_network_watcher	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36743	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-36785	microsoft - multiple products	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2023-10-10	7.8	High
CVE-2023-36790	microsoft - multiple products	Windows RDP Encoder Mirror Driver Elevation of Privilege Vulnerability	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
CVE-2023-41772	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7.8	High
CVE-2023-26370	adobe - multiple products	Adobe Photoshop versions 23.5.5 (and earlier) and 24.7 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-10-11	7.8	High
CVE-2023-40141	google - android	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 execution privileges needed. User interaction is not needed for exploitation.	2023-10-11	7.8	High
CVE-2023-40142	google - android	In TBD of TBD, there is a possible way to bypass carrier restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-11	7.8	High
CVE-2023-3781	google - android	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 exploitation.	2023-10-11	7.8	High
CVE-2023-32722	zabbix - multiple products	The zabbix/src/libs/zbxjson module is vulnerable to a buffer overflow when parsing JSON files via zbx_json_open.	2023-10-12	7.8	High
CVE-2023-27316	netapp - snapcenter	SnapCenter versions 4.8 through 4.9 are susceptible to a vulnerability which may allow an authenticated SnapCenter Server user to	2023-10-12	7.8	High

		become an admin user on a remote system where a SnapCenter plug-in has been installed.			
CVE-2023-44194	juniper - multiple products	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.	2023-10-13	7.8	High
CVE-2023-43079	dell - emc_openmanage_server_administrator	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
CVE-2023-35024	ibm - multiple products	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 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	2023-10-08	7.5	High
CVE-2023-40310	sap - powerdesigner	SAP PowerDesigner Client - version 16.7, does not sufficiently validate BPMN2 XML document imported from an untrusted 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.	2023-10-10	7.5	High
CVE-2023-40534	f5 - multiple products	When a client-side HTTP/2 profile and the HTTP MRF Router 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
CVE-2023-41085	f5 - multiple products	When IPSec is configured on a Virtual Server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	7.5	High
CVE-2023-4966	citrix - multiple products	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	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

CVE-2023-40718	fortinet - fortios_ips_engine	A interpretation conflict in Fortinet IPS Engine versions 7.321, 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
CVE-2023-36438	microsoft - multiple products	Windows TCP/IP Information Disclosure Vulnerability	2023-10-10	7.5	High
CVE-2023-36567	microsoft - multiple products	Windows Deployment Services Information Disclosure Vulnerability	2023-10-10	7.5	High
CVE-2023-36579	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36581	microsoft - multiple 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
CVE-2023-36606	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36703	microsoft - multiple products	DHCP Server Service Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36707	microsoft - multiple products	Windows Deployment Services Denial of Service Vulnerability	2023-10-10	7.5	High
CVE-2023-36709	microsoft - multiple 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
CVE-2023-42794	apache - multiple products	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. Users are recommended to upgrade to version 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.	2023-10-10	7.5	High
CVE-2023-44093	huawei - multiple products	Vulnerability of package names' public keys not being verified in the security module.Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVE-2023-44096	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
CVE-2023-44109	huawei - multiple products	Clone vulnerability in the huks ta module.Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVE-2023-44095	huawei - multiple products	Use-After-Free (UAF) vulnerability in the surfaceflinger module.Successful exploitation of this vulnerability can cause system crash.	2023-10-11	7.5	High
CVE-2023-44097	huawei - multiple products	Vulnerability of the permission to access device SNs being improperly managed.Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVE-2023-44100	huawei - multiple products	Broadcast permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVE-2023-44101	huawei - multiple products	The Bluetooth module has a vulnerability in permission control for broadcast notifications.Successful exploitation of this vulnerability may affect confidentiality.	2023-10-11	7.5	High
CVE-2023-44103	huawei - multiple products	Out-of-bounds read vulnerability in the Bluetooth module.Successful exploitation of this vulnerability may affect service confidentiality.	2023-10-11	7.5	High
CVE-2023-44104	huawei - multiple products	Broadcast permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability may affect 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
CVE-2023-44108	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	7.5	High
CVE-2023-44114	huawei - multiple products	Out-of-bounds array vulnerability in the dataipa module.Successful 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.	2023-10-11	7.5	High
CVE-2023-35652	google - android	In ProtocolEmergencyCallListIndAdapter::Init of protocolcalladapter.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 required. User interaction is not needed for exploitation.	2023-10-11	7.5	High
CVE-2023-35661	google - android	In ProfSixDecomTcpSACKoption of RohcPacketCommon.cpp, there 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 needed for exploitation.	2023-10-11	7.5	High
CVE-2023-44186	juniper - multiple products	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.	2023-10-11	7.5	High
CVE-2023-27314	netapp - multiple products	ONTAP 9 versions prior to 9.8P19, 9.9.1P16, 9.10.1P12, 9.11.1P8, 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.			
CVE-2023-36841	juniper - multiple products	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;	2023-10-12	7.5	High
CVE-2023-36843	juniper - multiple products	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;	2023-10-12	7.5	High
CVE-2023-44175	juniper - multiple products	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. Note: This issue is not noticed when all the devices in the network are Juniper devices. This issue affects Juniper Networks:	2023-10-12	7.5	High

متاح

		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.			
CVE-2023-44181	juniper - multiple products	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 l2 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.	2023-10-13	7.5	High
CVE-2023-44185	juniper - multiple 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. 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; * 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

متاح

		Juniper Networks Junos OS Evolved: * 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.			
CVE-2023-44191	juniper - multiple products	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: Juniper Networks Junos OS on QFX5000 Series and EX4000 Series * 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. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1	2023-10-13	7.5	High
CVE-2023-44192	juniper - multiple products	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: * All versions prior to 20.4R3-S6; * 21.1 versions prior to 21.1R3-S5;	2023-10-13	7.5	High

متاح

		* 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 22.3R2-S1, 22.3R3; * 22.4 versions prior to 22.4R1-S2, 22.4R2.			
CVE-2023-44197	juniper - multiple products	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; * 21.4 versions prior to 21.4R2-S1, 21.4R3-S5. 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.	2023-10-13	7.5	High
CVE-2023-44198	juniper - multiple products	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.	2023-10-13	7.5	High

متاح

		This issue doesn't not affected releases prior to 20.4R1.			
CVE-2023-44199	juniper - multiple products	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: * 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.	2023-10-13	7.5	High
CVE-2023-38220	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 Authorization vulnerability that could lead in a security feature bypass in a way that an attacker could access unauthorised data. Exploitation of this issue does not require user interaction.	2023-10-13	7.5	High
CVE-2023-41682	fortinet - multiple products	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 2.5.0 through 2.5.2 and 2.4.1 and 2.4.0 allows attacker to denial of service via crafted http requests.	2023-10-13	7.5	High
CVE-2023-4499	hp - thinupdate	A potential security vulnerability has been identified in the HP 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 vulnerability.	2023-10-13	7.5	High
CVE-2023-32974	qnap - multiple products	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 QuTS hero h5.1.0.2424 build 20230609 and later QuTScloud c5.1.0.2498 and later	2023-10-13	7.5	High
CVE-2022-33165	ibm - security_directory_integrator	IBM Security Directory Server 6.4.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 228582.	2023-10-14	7.5	High
CVE-2022-43740	ibm - security_verify_access_oidc_provider	IBM Security Verify Access OIDC Provider could allow a remote user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 238921.	2023-10-14	7.5	High
CVE-2023-30994	ibm - multiple products	IBM QRadar SIEM 7.5.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 254138	2023-10-14	7.5	High
CVE-2023-45862	linux - linux_kernel	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 object could potentially extend beyond the end of an allocation.	2023-10-14	7.5	High
CVE-2023-45226	f5 - big-ip_next_service_proxy_for_kubernetes	The BIG-IP SPK TMM (Traffic Management Module) f5-debug-sidecar and f5-debug-sshd containers contains hardcoded credentials that may allow an attacker with the ability to intercept traffic to impersonate the SPK Secure Shell (SSH) server on those containers. This is only exposed when ssh debug is enabled. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2023-10-10	7.4	High
CVE-2023-36561	microsoft - multiple products	Azure DevOps Server Elevation of Privilege Vulnerability	2023-10-10	7.3	High
CVE-2023-36570	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High

متاح

CVE-2023-36571	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36572	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36573	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36574	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36575	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36578	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36582	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36583	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36589	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36590	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36591	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36592	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-36593	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-10-10	7.3	High
CVE-2023-42768	f5 - multiple products	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, tmsh, or iControl REST. BIG-IP non-admin user can still have access to iControl REST admin resource. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	7.2	High
CVE-2023-36780	microsoft - multiple products	Skype for Business Remote Code Execution Vulnerability	2023-10-10	7.2	High
CVE-2023-36786	microsoft - multiple products	Skype for Business Remote Code Execution Vulnerability	2023-10-10	7.2	High
CVE-2023-36789	microsoft - multiple products	Skype for Business Remote Code Execution Vulnerability	2023-10-10	7.2	High
CVE-2023-35649	google - android	In several functions of Exynos modem 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. User interaction is not needed for exploitation.	2023-10-11	7.2	High
CVE-2023-32973	qnap - multiple products	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 5.0.1.2425 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	2023-10-13	7.2	High
CVE-2023-32976	qnap - container_station	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. We have already fixed the vulnerability in the following version: Container Station 2.6.7.44 and later	2023-10-13	7.2	High
CVE-2023-41838	fortinet - multiple products	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.	2023-10-10	7.1	High
CVE-2023-36565	microsoft - multiple products	Microsoft Office Graphics Elevation of Privilege Vulnerability	2023-10-10	7	High
CVE-2023-36568	microsoft - multiple products	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	2023-10-10	7	High
CVE-2023-36721	microsoft - multiple products	Windows Error Reporting Service Elevation of Privilege Vulnerability	2023-10-10	7	High
CVE-2023-36776	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2023-10-10	7	High
CVE-2023-36902	microsoft - multiple products	Windows Runtime Remote Code Execution Vulnerability	2023-10-10	7	High
CVE-2023-38159	microsoft - multiple products	Windows Graphics Component Elevation of Privilege Vulnerability	2023-10-10	7	High

CVE-2022-3728	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
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
CVE-2022-48183	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
CVE-2023-26366	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 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.	2023-10-13	6.8	Medium
CVE-2023-5409	hp - t430_thin_client_firmware	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 providing recommended guidance for customers to reduce exposure to the potential vulnerability.	2023-10-13	6.8	Medium
CVE-2023-40653	google - android	In FW-PackageManager, there is a possible missing permission check. This could lead to local escalation of privilege with System execution privileges needed	2023-10-08	6.7	Medium
CVE-2023-40654	google - android	In FW-PackageManager, there is a possible missing permission 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_firmware	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-2023-35654	google - android	In ctrl_roi of stmvl53l1_module.c, there is a possible out of bounds 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.	2023-10-11	6.7	Medium
CVE-2023-35655	google - android	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 execution privileges needed. User interaction is not needed for exploitation.	2023-10-11	6.7	Medium
CVE-2023-35660	google - android	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 lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-11	6.7	Medium
CVE-2023-38221	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 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
CVE-2023-38249	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 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
CVE-2023-38250	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 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	2023-10-13	6.6	Medium

متاح

		interaction and attack complexity is high as it requires knowledge of tooling beyond just using the UI.			
CVE-2023-42477	sap - netweaver_application_server_java	SAP NetWeaver AS Java (GRMG Heartbeat application) - version 7.50, allows an attacker to send a crafted request from a vulnerable web application, causing limited impact on confidentiality and integrity of the application.	2023-10-10	6.5	Medium
CVE-2023-41964	f5 - multiple products	The BIG-IP and BIG-IQ systems do not encrypt some sensitive information written to Database (DB) variables. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	6.5	Medium
CVE-2023-42787	fortinet - multiple products	A client-side enforcement of server-side security [CWE-602] 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 remote attacker with low privileges to access a privileged web console via client side code execution.	2023-10-10	6.5	Medium
CVE-2023-44249	fortinet - multiple products	An authorization bypass through user-controlled key [CWE-639] 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 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
CVE-2023-36433	microsoft - multiple products	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36563	microsoft - multiple products	Microsoft WordPad Information Disclosure Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36564	microsoft - multiple products	Windows Search Security Feature Bypass Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36566	microsoft - multiple products	Microsoft Common Data Model SDK Denial of Service Vulnerability	2023-10-10	6.5	Medium
CVE-2023-36706	microsoft - multiple products	Windows Deployment Services Information Disclosure 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
CVE-2023-5475	google - chrome	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 via a crafted Chrome Extension. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
CVE-2023-5479	google - chrome	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 crafted HTML page. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
CVE-2023-5481	google - chrome	Inappropriate implementation in Downloads in 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
CVE-2023-5483	google - chrome	Inappropriate implementation in Intents in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
CVE-2023-5484	google - chrome	Inappropriate implementation in Navigation in 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
CVE-2023-5487	google - chrome	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 a crafted Chrome Extension. (Chromium security severity: Medium)	2023-10-11	6.5	Medium
CVE-2023-22392	juniper - multiple products	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. 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

		expr_dfw_hw_sfm_add:750 Unable to add the filter secondarymatch to the hardware expr_dfw_base_hw_add:52 Failed to add h/w sfm data. expr_dfw_base_hw_create:114 Failed to add h/w data. expr_dfw_base_pfe_inst_create:241 Failed to create base inst for sfilter 0 on PFE 0 for __flowspec_default_inet__ expr_dfw_flt_inst_change:1368 Failed to create __flowspec_default_inet__ on PFE 0 expr_dfw_hw_pgm_fnum:465 dfw_pfe_inst_old not found for pfe_index 0! expr_dfw_bp_pgm_flt_num:548 Failed to pgm bind-point in hw: generic failure expr_dfw_bp_topo_handler:1102 Failed to program fnum. expr_dfw_entry_process_change:679 Failed to change instance for filter __flowspec_default_inet__. This issue affects Juniper Networks Junos OS: on PTX1000, PTX10002, and PTX10004, PTX10008 and PTX10016 with LC110x FPCs: * All versions prior to 20.4R3-S5; * 21.1 versions prior to 21.1R3-S4; * 21.2 versions prior to 21.2R3-S2; * 21.3 versions prior to 21.3R3; * 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 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-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-2023-36839	juniper - multiple products	An Improper Validation of Specified Quantity in Input vulnerability in the Layer-2 control protocols daemon (l2cpd) 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 l2cpd 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 22.1R3-S2; * 22.2 versions prior to 22.2R3; * 22.3 versions prior to 22.3R2-S2; * 22.4 versions prior to 22.4R2;	2023-10-12	6.5	Medium

متاح

		Juniper Networks Junos OS Evolved * 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;			
CVE-2023-44184	juniper - multiple products	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. Juniper Networks Junos OS Evolved * 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'" For example:	2023-10-13	6.5	Medium

متاح

		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'			
CVE-2023-44196	juniper - multiple products	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.	2023-10-13	6.5	Medium
CVE-2023-44203	juniper - multiple products	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.	2023-10-13	6.5	Medium
CVE-2023-44204	juniper - multiple products	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	2023-10-13	6.5	Medium

متاح

		* 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
CVE-2023-42780	apache - airflow	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. 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
CVE-2023-42792	apache - airflow	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 2.7.2 or newer to mitigate the risk associated with this vulnerability.	2023-10-14	6.5	Medium
CVE-2023-35645	google - android	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 needed for exploitation.	2023-10-11	6.4	Medium
CVE-2023-45863	linux - linux_kernel	An issue was discovered in lib/kobject.c in the Linux kernel before 6.2.3. With root access, an attacker can trigger a race condition that results in a fill_kobj_path out-of-bounds write.	2023-10-14	6.4	Medium
CVE-2023-5473	google - chrome	Use after free in Cast in Google Chrome prior to 118.0.5993.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	2023-10-11	6.3	Medium
CVE-2023-36416	microsoft - multiple products	Microsoft Dynamics 365 (on-premises) Cross-site Scripting 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.	2023-10-13	6.1	Medium
CVE-2023-41836	fortinet - multiple products	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 attacker to execute unauthorized code or commands via crafted HTTP requests.	2023-10-13	6.1	Medium

CVE-2023-39189	linux - 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, leading to a crash or information disclosure.	2023-10-09	6	Medium
CVE-2023-39192	linux - linux_kernel	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 the array boundaries, leading to a crash or information disclosure.	2023-10-09	6	Medium
CVE-2023-39193	linux - linux_kernel	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 allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.	2023-10-09	6	Medium
CVE-2022-33161	ibm - multiple products	IBM Security Directory Server 6.4.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. X-Force ID: 228569.	2023-10-14	5.9	Medium
CVE-2023-40633	google - multiple products	In phasecheckserver, 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-2023-40637	google - multiple products	In telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-10-08	5.5	Medium
CVE-2023-40639	google - android	In SoundRecorder service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-10-08	5.5	Medium
CVE-2023-40640	google - android	In SoundRecorder service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-10-08	5.5	Medium
CVE-2023-40641	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	2023-10-08	5.5	Medium
CVE-2023-40642	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	2023-10-08	5.5	Medium
CVE-2023-40643	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	2023-10-08	5.5	Medium
CVE-2023-40644	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	2023-10-08	5.5	Medium
CVE-2023-40645	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	2023-10-08	5.5	Medium
CVE-2023-40646	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	2023-10-08	5.5	Medium
CVE-2023-40647	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	2023-10-08	5.5	Medium
CVE-2023-40648	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	2023-10-08	5.5	Medium
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	2023-10-08	5.5	Medium
CVE-2023-40650	google - multiple products	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	5.5	Medium
CVE-2023-41253	f5 - multiple products	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.	2023-10-10	5.5	Medium
CVE-2023-43485	f5 - multiple products	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.	2023-10-10	5.5	Medium
CVE-2023-25604	fortinet - fortiguest	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.	2023-10-10	5.5	Medium
CVE-2023-36576	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	2023-10-10	5.5	Medium
CVE-2023-36713	microsoft - multiple products	Windows Common Log File System Driver Information Disclosure Vulnerability	2023-10-10	5.5	Medium

CVE-2023-36724	microsoft - multiple products	Windows Power Management Service Information Disclosure 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
CVE-2023-38216	adobe - multiple 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 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.	2023-10-11	5.5	Medium
CVE-2023-44187	juniper - multiple products	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. 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.	2023-10-11	5.5	Medium
CVE-2023-27315	netapp - snapgathers	SnapGathers versions prior to 4.9 are susceptible to a vulnerability which could allow a local authenticated attacker to discover plaintext domain user credentials	2023-10-12	5.5	Medium
CVE-2023-44176	juniper - multiple products	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.	2023-10-13	5.5	Medium
CVE-2023-44177	juniper - multiple products	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: * 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

متاح

		* 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; * 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.			
CVE-2023-44178	juniper - multiple products	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.	2023-10-13	5.5	Medium
CVE-2023-44193	juniper - multiple products	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: 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.			
CVE-2023-44201	juniper - multiple products	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: Juniper Networks Junos OS * 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. Juniper Networks Junos OS Evolved * 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.	2023-10-13	5.5	Medium
CVE-2023-42752	linux - linux_kernel	An integer overflow flaw was found in the Linux kernel. This issue leads to the kernel allocating `skb_shared_info` in the userspace, which is exploitable in systems without SMAP protection since `skb_shared_info` contains references to function pointers.	2023-10-13	5.5	Medium
CVE-2023-45176	ibm - multiple products	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 Windows. IBM X-Force ID: 247998.	2023-10-14	5.5	Medium
CVE-2023-42473	sap - s\/4hana	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.	2023-10-10	5.4	Medium
CVE-2023-42474	sap - businessobjects_web_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.	2023-10-10	5.4	Medium
CVE-2023-44315	siemens - sinec_nms	A vulnerability has been identified in SINEC NMS (All versions < V2.0). The affected application improperly sanitizes certain SNMP 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.	2023-10-10	5.4	Medium
CVE-2023-36555	fortinet - fortios	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

متاح

		to execute unauthorized code or commands via the SAML and Security Fabric components.			
CVE-2023-36637	fortinet - multiple products	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiMail version 7.2.0 through 7.2.2 and before 7.0.5 allows an authenticated attacker to inject HTML tags 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
CVE-2023-44189	juniper - multiple products	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 Juniper Networks Junos OS Evolved on PTX10003 Series: * 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.	2023-10-11	5.4	Medium
CVE-2023-44190	juniper - multiple products	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 issue affects Juniper Networks Junos OS Evolved on PTX10001, PTX10004, PTX10008, and PTX10016: * 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.	2023-10-11	5.4	Medium
CVE-2023-32721	zabbix - multiple products	A stored XSS has been found in the Zabbix web application in the Maps element if a URL field is set with spaces before URL.	2023-10-12	5.4	Medium
CVE-2023-38000	wordpress - multiple products	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.	2023-10-13	5.4	Medium
CVE-2023-41843	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 allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2023-10-13	5.4	Medium
CVE-2023-34977	qnap - video_station	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: Video Station 5.7.0 (2023/07/27) and later	2023-10-13	5.4	Medium
CVE-2023-40367	ibm - multiple products	IBM QRadar SIEM 7.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the	2023-10-14	5.4	Medium

		Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 263376.			
CVE-2023-41675	fortinet - multiple products	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 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 inspection.	2023-10-10	5.3	Medium
CVE-2023-42782	fortinet - multiple products	A insufficient verification of data authenticity vulnerability [CWE-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 serial number.	2023-10-10	5.3	Medium
CVE-2023-41763	microsoft - multiple products	Skype for Business Elevation of Privilege Vulnerability	2023-10-10	5.3	Medium
CVE-2023-42795	apache - multiple products	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 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, which fixes the issue.	2023-10-10	5.3	Medium
CVE-2023-45648	apache - multiple products	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. 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
CVE-2023-41304	huawei - multiple products	Parameter verification vulnerability in the window module.Successful exploitation of this vulnerability may cause the size of an app window to be adjusted to that of a floating window.	2023-10-11	5.3	Medium
CVE-2023-44102	huawei - multiple products	Broadcast permission control vulnerability in the Bluetooth module.Successful exploitation of this vulnerability can cause the Bluetooth function to be unavailable.	2023-10-11	5.3	Medium
CVE-2023-44188	juniper - multiple products	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: * 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

		* 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.			
CVE-2023-44183	juniper - multiple products	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 FPC0 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 FPC0 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.	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_access_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-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.	2023-10-13	4.9	Medium
CVE-2023-32970	qnap - multiple products	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. 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

متاح

CVE-2023-40631	google - multiple products	In Dialer, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	2023-10-08	4.4	Medium
CVE-2023-40636	google - android	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 privileges needed	2023-10-08	4.4	Medium
CVE-2023-40638	google - android	In Telecom service, there is a possible missing permission check. This could lead to local denial of service with System execution privileges needed	2023-10-08	4.4	Medium
CVE-2023-40651	google - multiple products	In urild service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-10-08	4.4	Medium
CVE-2023-40652	google - android	In jpg driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	2023-10-08	4.4	Medium
CVE-2023-39194	linux - multiple products	A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of state filters, which can 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-bounds read, potentially leading to an information disclosure.	2023-10-09	4.4	Medium
CVE-2023-37195	siemens - simatic_cp_1604_firmware	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 allow local attackers with administrative privileges to cause a denial of service situation on the host. A physical power cycle is required to get the system working again.	2023-10-10	4.4	Medium
CVE-2023-38640	siemens - sicam_pas\/pqs	A vulnerability has been identified in SICAM PAS/PQS (All versions >= V8.00 < V8.22). The affected application is installed with specific files and folders with insecure permissions. This could 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-2023-39447	f5 - multiple products	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.	2023-10-10	4.4	Medium
CVE-2023-45219	f5 - multiple products	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. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-10-10	4.4	Medium
CVE-2023-36698	microsoft - multiple 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
CVE-2023-35653	google - android	In TBD of TBD, there is a possible way to access location information due to a permissions bypass. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2023-10-11	4.4	Medium
CVE-2023-40682	ibm - app_connect_enterprise	IBM App Connect Enterprise 12.0.1.0 through 12.0.8.0 contains an unspecified vulnerability that could allow a local privileged user to obtain sensitive information from API logs. IBM X-Force ID: 263833.	2023-10-13	4.4	Medium
CVE-2023-41365	sap - business_one	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 and availability.	2023-10-10	4.3	Medium
CVE-2023-42475	sap - multiple products	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-2023-33301	fortinet - multiple products	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 from a non trusted host.	2023-10-10	4.3	Medium
CVE-2023-44110	huawei - multiple products	Out-of-bounds access vulnerability in the audio module.Successful exploitation of this vulnerability may affect availability.	2023-10-11	4.3	Medium

CVE-2023-5477	google - chrome	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 severity: Low)	2023-10-11	4.3	Medium
CVE-2023-5478	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2023-10-11	4.3	Medium
CVE-2023-5485	google - chrome	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: Low)	2023-10-11	4.3	Medium
CVE-2023-5486	google - chrome	Inappropriate implementation in Input in Google Chrome prior to 118.0.5993.70 allowed a remote attacker to spoof security UI via a crafted HTML page. (Chromium security severity: Low)	2023-10-11	4.3	Medium
CVE-2023-27312	netapp - snapcenter_plug-in	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 VMware vSphere user interface.	2023-10-12	4.3	Medium
CVE-2023-39999	wordpress - multiple products	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, from 4.5 through 4.5.29, from 4.4 through 4.4.30, from 4.3 through 4.3.31, from 4.2 through 4.2.35, from 4.1 through 4.1.38.	2023-10-13	4.3	Medium
CVE-2023-45348	apache - airflow	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 default. It is recommended to upgrade to a version that is not affected.	2023-10-14	4.3	Medium
CVE-2023-36559	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2023-10-13	4.2	Medium
CVE-2023-37939	fortinet - multiple products	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 local authenticated attacker with no Administrative privileges to retrieve the list of files or folders excluded from malware scanning.	2023-10-10	3.3	Low
CVE-2023-5449	hp - e22_g4_fhd_firmware	A potential security vulnerability has been identified in certain HP Displays supporting the Theft Deterrence feature which may allow a monitor's Theft Deterrence to be deactivated.	2023-10-13	3.3	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.