الهيئة الوطنية للأمن السيبراني
Nat onal Cybersecurity Authority

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

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

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 7th of January to 14th of January. 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**

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 ٧ يناير إلى ١٤ يناير ٢٠٢٤. 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-50948	ibm - storage_fusion_hci	IBM Storage Fusion HCI 2.1.0 through 2.6.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 275671.	2024-01-08	9.8	Critical
CVE-2024-21646	microsoft - azure_uamqp	Azure uAMQP is a general purpose C library for AMQP 1.0. The UAMQP library is used by several clients to implement AMQP protocol communication. When clients using this library receive a crafted binary type data, an integer overflow or wraparound or memory safety issue can occur and may cause remote code execution. This vulnerability has been patched in release 2024-01-01.	2024-01-09	9.8	Critical
CVE-2023-49235	trendnet - tv-ip1314pi_firmware	An issue was discovered in libremote_dbg.so on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Filtering of debug information is mishandled during use of popen. Consequently, an attacker can bypass validation and execute a shell command.	2024-01-09	9.8	Critical
CVE-2023-49236	trendnet - tv-ip1314pi_firmware	A stack-based buffer overflow was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices, leading to arbitrary command execution. This occurs because of lack of length validation during an sscanf of a user-entered scale field in the RTSP playback function of davinci.	2024-01-09	9.8	Critical
CVE-2023-49237	trendnet - tv-ip1314pi_firmware	An issue was discovered on TRENDnet TV-IP1314PI 5.5.3 200714 devices. Command injection can occur because the system function is used by davinci to unpack language packs without strict filtering of URL strings.	2024-01-09	9.8	Critical
CVE-2023-49251	siemens - simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application allows an attacker to add their own login credentials to the device. This allows an attacker to remotely login as root and take control of the device even after the affected device is fully set up.	2024-01-09	9.8	Critical
CVE-2023-49621	siemens - simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The "intermediate installation" system state of the affected application uses default credential with admin privileges. An attacker could use the credentials to gain complete control of the affected device.	2024-01-09	9.8	Critical
CVE-2024-0057	microsoft - multiple products	NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability	2024-01-09	9.8	Critical
CVE-2023-31488	cisco - ironport_email_security_appliance	Hyland Perceptive Filters releases before 2023-12-08 (e.g., 11.4.0.2647), as used in Cisco IronPort Email Security Appliance Software, Cisco Secure Email Gateway, and various non-Cisco products, allow attackers to trigger a segmentation fault and execute arbitrary code via a crafted document.	2024-01-10	9.8	Critical
CVE-2023-40414	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 10, iOS 17 and iPadOS 17, tvOS 17, macOS Sonoma 14, Safari 17. Processing web content may lead to arbitrary code execution.	2024-01-10	9.8	Critical

CVE-2024-21638	microsoft - azure_ipam	Azure IPAM (IP Address Management) is a lightweight solution developed on top of the Azure platform designed to help Azure customers manage their IP Address space easily and effectively. By design there is no write access to customers' Azure environments as the Service Principal used is only assigned the Reader role at the root Management Group level. Until recently, the solution lacked the validation of the passed in authentication token which may result in attacker impersonating any privileged user to access data stored within the IPAM instance and subsequently from Azure, causing an elevation of privilege. This vulnerability has been patched in version 3.0.0.	2024-01-10	9.8	Critical

CVE-2024-21591	juniper - multiple products	An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device.
		This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory.
		This issue affects Juniper Networks Junos OS SRX Series and EX Series:
		* Junos OS versions earlier than 20.4R3-S9;
		* Junos OS 21.2 versions earlier than 21.2R3-S7;
		* Junos OS 21.3 versions earlier than 21.3R3-S5;
		* Junos OS 21.4 versions earlier than 21.4R3-S5;
		* Junos OS 22.1 versions earlier than 22.1R3-S4;
		* Junos OS 22.2 versions earlier than 22.2R3-S3;
		* Junos OS 22.3 versions earlier than 22.3R3-S2;
		* Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3.
			2024-01-12	9.8	Critical

CVE-2024-21737	sap - application_interface_framework	In SAP Application Interface Framework File Adapter - version 702, a high privilege user can use a function module to traverse through various layers and execute OS commands directly. By this, such user can control the behaviour of the application. This leads to considerable impact on confidentiality, integrity and availability.	2024-01-09	9.1	Critical
CVE-2024-21887	ivanti - multiple products	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.	2024-01-12	9.1	Critical
CVE-2023-39336	ivanti - multiple products	An unspecified SQL Injection vulnerability in Ivanti Endpoint Manager released prior to 2022 SU 5 allows an attacker with access to the internal network to execute arbitrary SQL queries and retrieve output without the need for authentication. Under specific circumstances, this may also lead to RCE on the core server.	2024-01-09	8.8	High
CVE-2024-20674	microsoft - multiple products	Windows Kerberos Security Feature Bypass Vulnerability	2024-01-09	8.8	High
CVE-2024-21318	microsoft - multiple products	Microsoft SharePoint Server Remote Code Execution Vulnerability	2024-01-09	8.8	High
CVE-2024-21643	microsoft - multiple products	IdentityModel Extensions for .NET provide assemblies for web developers that wish to use federated identity providers for establishing the caller's identity. Anyone leveraging the `SignedHttpRequest`protocol or the `SignedHttpRequestValidator`is vulnerable. Microsoft.IdentityModel trusts the `jku`claim by default for the `SignedHttpRequest`protocol. This raises the possibility to make any remote or local `HTTP GET` request. The vulnerability has been fixed in Microsoft.IdentityModel.Protocols.SignedHttpRequest. Users should update all their Microsoft.IdentityModel versions to 7.1.2 (for 7x) or higher, 6.34.0 (for 6x) or higher.	2024-01-10	8.8	High
CVE-2023-44250	fortinet - multiple products	An improper privilege management vulnerability [CWE-269] in a Fortinet FortiOS HA cluster version 7.4.0 through 7.4.1 and 7.2.5 and in a FortiProxy HA cluster version 7.4.0 through 7.4.1 allows an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.	2024-01-10	8.8	High
CVE-2023-46712	fortinet - multiple products	A improper access control in Fortinet FortiPortal version 7.0.0 through 7.0.6, Fortinet FortiPortal version 7.2.0 through 7.2.1 allows attacker to escalate its privilege via specifically crafted HTTP requests.	2024-01-10	8.8	High

CVE-2023-41060	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. A remote user may be able to cause kernel code execution.	2024-01-10	8.8	High
CVE-2023-42833	apple - multiple products	A correctness issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14, Safari 17, iOS 17 and iPadOS 17. Processing web content may lead to arbitrary code execution.	2024-01-10	8.8	High
CVE-2023-42866	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.5, iOS 16.6 and iPadOS 16.6, tvOS 16.6, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	2024-01-10	8.8	High
CVE-2024-21773	tp-link - archer_ax3000_firmware	Multiple TP-LINK products allow a network-adjacent unauthenticated attacker with access to the product to execute arbitrary OS commands. Affected products/versions are as follows: Archer AX3000 firmware versions prior to "Archer AX3000(JP)_V1_1.1.2 Build 20231115", Archer AX5400 firmware versions prior to "Archer AX5400(JP)_V1_1.1.2 Build 20231115", Deco X50 firmware versions prior to "Deco X50(JP)_V1_1.4.1 Build 20231122", and Deco XE200 firmware versions prior to "Deco XE200(JP)_V1_1.2.5 Build 20231120".	2024-01-11	8.8	High
CVE-2024-21833	tp-link - archer_ax3000_firmware	Multiple TP-LINK products allow a network-adjacent unauthenticated attacker with access to the product to execute arbitrary OS commands. Affected products/versions are as follows: Archer AX3000 firmware versions prior to "Archer AX3000(JP)_V1_1.1.2 Build 20231115", Archer AX5400 firmware versions prior to "Archer AX5400(JP)_V1_1.1.2 Build 20231115", Archer AXE75 firmware versions prior to "Archer AXE75(JP)_V1_231115", Deco X50 firmware versions prior to "Deco X50(JP)_V1_1.4.1 Build 20231122", and Deco XE200 firmware versions prior to "Deco XE200(JP)_V1_1.2.5 Build 20231120".	2024-01-11	8.8	High
CVE-2024-0252	zohocorp - multiple products	ManageEngine ADSelfService Plus versions 6401 and below are vulnerable to the remote code execution due to the improper handling in the load balancer component. Authentication is required in order to exploit this vulnerability.	2024-01-11	8.8	High
CVE-2024-0056	microsoft - multiple products	Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability	2024-01-09	8.7	High
CVE-2023-47211	zohocorp - multiple products	A directory traversal vulnerability exists in the uploadMib functionality of ManageEngine OpManager 12.7.258. A specially crafted HTTP request can lead to arbitrary file creation. An attacker can send a malicious MiB file to trigger this vulnerability.	2024-01-08	8.6	High
CVE-2023-46805	ivanti - multiple products	An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.	2024-01-12	8.2	High
CVE-2023-47140	ibm - cics_transaction_gateway	IBM CICS Transaction Gateway 9.3 could allow a user to transfer or view files due to improper access controls. IBM X-Force ID: 270259.	2024-01-08	8.1	High
CVE-2024-20652	microsoft - multiple products	Windows HTML Platforms Security Feature Bypass Vulnerability	2024-01-09	8.1	High
CVE-2023-51780	linux - multiple products	An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl in net/atm/ioctl.c has a use-after-free because of a vcc_recvmsg race condition.	2024-01-11	8.1	High
CVE-2024-20654	microsoft - multiple products	Microsoft ODBC Driver Remote Code Execution Vulnerability	2024-01-09	8	High
CVE-2024-20676	microsoft - azure_storage_mover	Azure Storage Mover Remote Code Execution Vulnerability	2024-01-09	8	High
CVE-2024-21821	tp-link - archer_ax3000_firmware	Multiple TP-LINK products allow a network-adjacent authenticated attacker to execute arbitrary OS commands. Affected products/versions are as follows: Archer AX3000 firmware versions prior to "Archer AX3000(JP)_V1_1.1.2 Build 20231115", Archer AX5400 firmware versions prior to "Archer AX5400(JP)_V1_1.1.2 Build 20231115", and Archer AXE75 firmware versions prior to "Archer AXE75(JP)_V1_231115".	2024-01-11	8	High
CVE-2023-47145	ibm - multiple products	IBM Db2 for Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow a local user to escalate their privileges to the SYSTEM user using the MSI repair functionality. IBM X-Force ID: 270402.	2024-01-07	7.8	High
CVE-2022-2585	linux - linux_kernel	It was discovered that when exec'ing from a non-leader thread, armed POSIX CPU timers would be left on a list but freed, leading to a use-after-free.	2024-01-08	7.8	High
CVE-2022-2586	linux - linux_kernel	It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted.	2024-01-08	7.8	High
CVE-2022-2588	linux - linux_kernel	It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0.	2024-01-08	7.8	High
CVE-2021-3600	linux - multiple products	It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers	2024-01-08	7.8	High

		when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code.			
CVE-2023-44120	siemens - spectrum_power_7	A vulnerability has been identified in Spectrum Power 7 (All versions < V23Q4). The affected product's sudo configuration permits the local administrative account to execute several entries as root user. This could allow an authenticated local attacker to inject arbitrary code and gain root access.	2024-01-09	7.8	High
CVE-2023-49121	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49122	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49123	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49124	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49126	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49127	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49128	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49129	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected applications contain a stack overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49130	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49131	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-49132	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 10). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-51439	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2023-51745	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could	2024-01-09	7.8	High

		allow an attacker to execute code in the context of the current process.			
CVE-2023-51746	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a stack overflow vulnerability while parsing specially crafted CGM files. This could allow an attacker to execute code in the context of the current process.	2024-01-09	7.8	High
CVE-2024-0206	trellix - anti-malware_engine	A symbolic link manipulation vulnerability in Trellix Anti-Malware Engine prior to the January 2024 release allows an authenticated local user to potentially gain an escalation of privileges. This was achieved by adding an entry to the registry under the Trellix ENS registry folder with a symbolic link to files that the user wouldn't normally have permission to. After a scan, the Engine would follow the links and remove the files	2024-01-09	7.8	High
CVE-2024-0213	trellix - multiple products	A buffer overflow vulnerability in TA for Linux and TA for MacOS prior to 5.8.1 allows a local user to gain elevated permissions, or cause a Denial of Service (DoS), through exploiting a memory corruption issue in the TA service, which runs as root. This may also result in the disabling of event reporting to ePO, caused by failure to validate input from the file correctly.	2024-01-09	7.8	High
CVE-2022-48618	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.1, watchOS 9.2, iOS 16.2 and iPadOS 16.2, tvOS 16.2. An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. Apple is aware of a report that this issue may have been exploited against versions of iOS released before iOS 15.7.1.	2024-01-09	7.8	High
CVE-2024-20653	microsoft - multiple products	Microsoft Common Log File System Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-20656	microsoft - multiple products	Visual Studio Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-20658	microsoft - multiple products	Microsoft Virtual Hard Disk Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-20677	microsoft - multiple products	<p>A security vulnerability exists in FBX that could lead to remote code execution. To mitigate this vulnerability, the ability to insert FBX files has been disabled in Word, Excel, PowerPoint and Outlook for Windows and Mac. Versions of Office that had this feature enabled will no longer have access to it. This includes Office 2019, Office 2021, Office LTSC for Mac 2021, and Microsoft 365.</p> <p>3D models in Office documents that were previously inserted from a FBX file will continue to work as expected unless the Link to File option was chosen at insert time.</p> <p>This change is effective as of the January 9, 2024 security update.</p>	2024-01-09	7.8	High
CVE-2024-20681	microsoft - multiple products	Windows Subsystem for Linux Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-20682	microsoft - multiple products	Windows Cryptographic Services Remote Code Execution Vulnerability	2024-01-09	7.8	High
CVE-2024-20683	microsoft - multiple products	Win32k Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-20686	microsoft - windows_server_2022_23h2	Win32k Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-20698	microsoft - multiple products	Windows Kernel Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-21309	microsoft - multiple products	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-21310	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2024-01-09	7.8	High
CVE-2024-21325	microsoft - printer_metadata_troubleshooter_tool	Microsoft Printer Metadata Troubleshooter Tool Remote Code Execution Vulnerability	2024-01-09	7.8	High
CVE-2023-7032	schneider-electric - easergy_studio	A CWE-502: Deserialization of untrusted data vulnerability exists that could allow an attacker logged in with a user level account to gain higher privileges by providing a harmful serialized object.	2024-01-09	7.8	High
CVE-2022-46721	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High

CVE-2022-47915	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2022-47965	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2023-32366	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4. Processing a font file may lead to arbitrary code execution.	2024-01-10	7.8	High
CVE-2023-32378	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2023-32383	apple - multiple products	This issue was addressed by forcing hardened runtime on the affected binaries at the system level. This issue is fixed in macOS Monterey 12.6.6, macOS Big Sur 11.7.7, macOS Ventura 13.4. An app may be able to inject code into sensitive binaries bundled with Xcode.	2024-01-10	7.8	High
CVE-2023-32401	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.6.6, macOS Big Sur 11.7.7, macOS Ventura 13.4. Parsing an office document may lead to an unexpected app termination or arbitrary code execution.	2024-01-10	7.8	High
CVE-2023-41075	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.5, macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4, iOS 15.7.4 and iPadOS 15.7.4, macOS Monterey 12.6.4. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2023-41974	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2023-42826	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to arbitrary code execution.	2024-01-10	7.8	High
CVE-2023-42828	apple - macos	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.5. An app may be able to gain root privileges.	2024-01-10	7.8	High
CVE-2023-42870	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2023-42871	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	2024-01-10	7.8	High
CVE-2023-42933	apple - macos	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to gain elevated privileges.	2024-01-10	7.8	High
CVE-2023-31003	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) could allow a local user to obtain root access due to improper access controls. IBM X-Force ID: 254658.	2024-01-11	7.8	High
CVE-2023-27098	tp-link - tapo	TP-Link Tapo APK up to v2.12.703 uses hardcoded credentials for access to the login panel.	2024-01-09	7.5	High
CVE-2024-22125	sap - gui_connector	Under certain conditions the Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge) - version 1.0, allows an attacker to access highly sensitive information which would otherwise be restricted causing high impact on confidentiality.	2024-01-09	7.5	High
CVE-2023-49252	siemens - simatic_cn_4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.7). The affected application allows IP configuration change without authentication to the device. This could allow an attacker to cause denial of service condition.	2024-01-09	7.5	High
CVE-2024-20661	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2024-01-09	7.5	High
CVE-2024-20672	microsoft - multiple products	.NET Denial of Service Vulnerability	2024-01-09	7.5	High
CVE-2024-20687	microsoft - multiple products	Microsoft AllJoyn API Denial of Service Vulnerability	2024-01-09	7.5	High
CVE-2024-20700	microsoft - multiple products	Windows Hyper-V Remote Code Execution Vulnerability	2024-01-09	7.5	High
CVE-2024-21307	microsoft - multiple products	Remote Desktop Client Remote Code Execution Vulnerability	2024-01-09	7.5	High
CVE-2024-21312	microsoft - .net_framework	.NET Framework Denial of Service Vulnerability	2024-01-09	7.5	High
CVE-2023-6476	redhat - openshift_container_platform	A flaw was found in CRI-O that involves an experimental annotation leading to a container being unconfined. This may allow a pod to specify and get any amount of memory/cpu, circumventing the kubernetes scheduler and potentially resulting in a denial of service in the node.	2024-01-09	7.5	High

CVE-2023-40393	apple - macos	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14. Photos in the Hidden Photos Album may be viewed without authentication.	2024-01-10	7.5	High
CVE-2023-42869	apple - multiple products	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Ventura 13.4, iOS 16.5 and iPadOS 16.5. Multiple issues in libxml2.	2024-01-10	7.5	High
CVE-2024-21589	juniper - multiple products	An Improper Access Control vulnerability in the Juniper Networks Paragon Active Assurance Control Center allows an unauthenticated network-based attacker to access reports without authenticating, potentially containing sensitive configuration information. A feature was introduced in version 3.1.0 of the Paragon Active Assurance Control Center which allows users to selectively share account data. By exploiting this vulnerability, it is possible to access reports without being logged in, resulting in the opportunity for malicious exfiltration of user data. Note that the Paragon Active Assurance Control Center SaaS offering is not affected by this issue. This issue affects Juniper Networks Paragon Active Assurance versions 3.1.0, 3.2.0, 3.2.2, 3.3.0, 3.3.1, 3.4.0. This issue does not affect Juniper Networks Paragon Active Assurance versions earlier than 3.1.0.	2024-01-12	7.5	High
CVE-2024-21595	juniper - multiple products	An Improper Validation of Syntactic Correctness of Input vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). If an attacker sends high rate of specific ICMP traffic to a device with VXLAN configured, this causes a deadlock of the PFE and results in the device becoming unresponsive. A manual restart will be required to recover the device. This issue only affects EX4100, EX4400, EX4600, QFX5000 Series devices. This issue affects: Juniper Networks Junos OS * 21.4R3 versions earlier than 21.4R3-S4; * 22.1R3 versions earlier than 22.1R3-S3; * 22.2R2 versions earlier than 22.2R3-S1; * 22.3 versions earlier than 22.3R2-S2, 22.3R3; * 22.4 versions earlier than 22.4R2; * 23.1 versions earlier than 23.1R2.	2024-01-12	7.5	High
CVE-2024-21597	juniper - multiple products	An Exposure of Resource to Wrong Sphere vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass the intended access restrictions. In an Abstracted Fabric (AF) scenario if routing-instances (RI) are configured, specific valid traffic destined to the device can bypass the configured lo0 firewall filters as it's received in the wrong RI context. This issue affects Juniper Networks Junos OS on MX Series: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R3;	2024-01-12	7.5	High

		* 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.			
CVE-2024-21602	juniper - multiple products	A NULL Pointer Dereference vulnerability in Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a specific IPv4 UDP packet is received and sent to the Routing Engine (RE) packetio crashes and restarts which causes a momentary traffic interruption. Continued receipt of such packets will lead to a sustained DoS. This issue does not happen with IPv6 packets. This issue affects Juniper Networks Junos OS Evolved on ACX7024, ACX7100-32C and ACX7100-48L: * 21.4-EVO versions earlier than 21.4R3-S6-EVO; * 22.1-EVO versions earlier than 22.1R3-S5-EVO; * 22.2-EVO versions earlier than 22.2R2-S1-EVO, 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions earlier than 21.4R1-EVO.	2024-01-12	7.5	High
CVE-2024-21604	juniper - multiple products	An Allocation of Resources Without Limits or Throttling vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). If a high rate of specific valid packets are processed by the routing engine (RE) this will lead to a loss of connectivity of the RE with other components of the chassis and thereby a complete and persistent system outage. Please note that a carefully designed lo0 firewall filter will block or limit these packets which should prevent this issue from occurring. The following log messages can be seen when this issue occurs: <host> kernel: nf_conntrack: nf_conntrack: table full, dropping packet This issue affects Juniper Networks Junos OS Evolved: * All versions earlier than 20.4R3-S7-EVO; * 21.2R1-EVO and later versions; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-EVO versions earlier than 22.1R3-S2-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO; * 22.3-EVO versions earlier than 22.3R2-EVO; * 22.4-EVO versions earlier than 22.4R2-EVO.	2024-01-12	7.5	High
CVE-2024-21606	juniper - multiple products	A Double Free vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). In a remote access VPN scenario, if a "tcp-encap-profile" is configured and a sequence of specific packets is received, a flowd crash and restart will be observed.	2024-01-12	7.5	High

		This issue affects Juniper Networks Junos OS on SRX Series:
		
		* All versions earlier than 20.4R3-S8;
		* 21.2 versions earlier than 21.2R3-S6;
		* 21.3 versions earlier than 21.3R3-S5;
		* 21.4 versions earlier than 21.4R3-S5;
		* 22.1 versions earlier than 22.1R3-S3;
		* 22.2 versions earlier than 22.2R3-S3;
		* 22.3 versions earlier than 22.3R3-S1;
		* 22.4 versions earlier than 22.4R2-S2, 22.4R3.			

CVE-2024-21611	juniper - multiple products	A Missing Release of Memory after Effective Lifetime 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). In a Juniper Flow Monitoring (jflow) scenario route churn that causes BGP next hops to be updated will cause a slow memory leak and eventually a crash and restart of rpd. Thread level memory utilization for the areas where the leak occurs can be checked using the below command: user@host> show task memory detail | match so_in so_in6 28 32 344450 11022400 344760 11032320 so_in 8 16 1841629 29466064 1841734 29467744 This issue affects: Junos OS * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Junos OS Evolved * 21.4-EVO versions earlier than 21.4R3-EVO; * 22.1-EVO versions earlier than 22.1R3-EVO; * 22.2-EVO versions earlier than 22.2R3-EVO. This issue does not affect: Juniper Networks Junos OS versions earlier than 21.4R1. Juniper Networks Junos OS Evolved versions earlier than 21.4R1.	2024-01-12	7.5	High
CVE-2024-21612	juniper - multiple products	An Improper Handling of Syntactically Invalid Structure vulnerability in Object Flooding Protocol (OFP) service of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On all Junos OS Evolved platforms, when specific TCP packets are received on an open OFP port, the OFP crashes leading to a restart of Routine Engine (RE). Continuous receipt of these specific TCP packets will lead to a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS Evolved	2024-01-12	7.5	High

		* All versions earlier than 21.2R3-S7-EVO; * 21.3 versions earlier than 21.3R3-S5-EVO ; * 21.4 versions earlier than 21.4R3-S5-EVO; * 22.1 versions earlier than 22.1R3-S4-EVO; * 22.2 versions earlier than 22.2R3-S3-EVO ; * 22.3 versions earlier than 22.3R3-EVO; * 22.4 versions earlier than 22.4R2-EVO, 22.4R3-EVO.			
CVE-2024-21614	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to cause rpd to crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when NETCONF and gRPC are enabled, and a specific query is executed via Dynamic Rendering (DREND), rpd will crash and restart. Continuous execution of this specific query will cause a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS * 22.2 versions earlier than 22.2R2-S2, 22.2R3; * 22.3 versions earlier than 22.3R2, 22.3R3. Juniper Networks Junos OS Evolved * 22.2 versions earlier than 22.2R2-S2-EVO, 22.2R3-EVO; * 22.3 versions earlier than 22.3R2-EVO, 22.3R3-EVO. This issue does not affect Juniper Networks: Junos OS versions earlier than 22.2R1; Junos OS Evolved versions earlier than 22.2R1-EVO.	2024-01-12	7.5	High
CVE-2024-21616	juniper - multiple products	An Improper Validation of Syntactic Correctness of Input vulnerability in Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On all Junos OS MX Series and SRX Series platforms, when SIP ALG is enabled, and a specific SIP packet is received and processed, NAT IP allocation fails for genuine traffic, which causes Denial of Service (DoS). Continuous receipt of this specific SIP ALG packet will cause a sustained DoS condition. NAT IP usage can be monitored by running the following command. user@srx> show security nat resource-usage source-pool <source_pool_name> Pool name: source_pool_name .. Address Factor-index Port-range Used Avail Total Usage X.X.X.X 0 Single Ports 50258 52342 62464 96% <<<< - Alg Ports 0 2048 2048 0%	2024-01-12	7.5	High

		This issue affects:
		Juniper Networks Junos OS on MX Series and SRX Series
		* All versions earlier than 21.2R3-S6;
		* 21.3 versions earlier than 21.3R3-S5;
		* 21.4 versions earlier than 21.4R3-S5;
		* 22.1 versions earlier than 22.1R3-S4;
		* 22.2 versions earlier than 22.2R3-S3;
		* 22.3 versions earlier than 22.3R3-S1;
		* 22.4 versions earlier than 22.4R2-S2, 22.4R3;
		* 23.2 versions earlier than 23.2R1-S1, 23.2R2.			

CVE-2023-0437	mongodb - c_driver	When calling bson_utf8_validate on some inputs a loop with an exit condition that cannot be reached may occur, i.e. an infinite loop. This issue affects All MongoDB C Driver versions prior to versions 1.25.0.	2024-01-12	7.5	High
CVE-2024-20696	microsoft - multiple products	Windows Libarchive Remote Code Execution Vulnerability	2024-01-09	7.3	High
CVE-2024-20697	microsoft - multiple products	Windows Libarchive Remote Code Execution Vulnerability	2024-01-09	7.3	High
CVE-2024-21735	sap - multiple products	SAP LT Replication Server - version S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, does not perform necessary authorization checks. This could allow an attacker with high privileges to perform unintended actions, resulting in escalation of privileges, which has High impact on confidentiality, integrity and availability of the system.	2024-01-09	7.2	High
CVE-2023-42797	siemens - sicam_a8000_cp-8050_firmware	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05.20), CP-8050 MASTER MODULE (All versions < CPCI85 V05.20). The network configuration service of affected devices contains a flaw in the conversion of ipv4 addresses that could lead to an uninitialized variable being used in succeeding validation steps. By uploading specially crafted network configuration, an authenticated remote attacker could be able to inject commands that are executed on the device with root privileges during device startup.	2024-01-09	7.2	High
CVE-2023-32436	apple - macos	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2024-01-10	7.1	High
CVE-2023-38610	apple - multiple products	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to cause unexpected system termination or write kernel memory.	2024-01-10	7.1	High
CVE-2023-42876	apple - macos	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	2024-01-10	7.1	High
CVE-2022-2602	linux - linux_kernel	io_uring UAF, Unix SCM garbage collection	2024-01-08	7	High
CVE-2024-20657	microsoft - multiple products	Windows Group Policy Elevation of Privilege Vulnerability	2024-01-09	7	High
CVE-2023-42832	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to gain root privileges.	2024-01-10	7	High
CVE-2023-51781	linux - multiple products	An issue was discovered in the Linux kernel before 6.6.8. atalk_ioctl in net/appletalk/ddp.c has a use-after-free because of an atalk_recvmsg race condition.	2024-01-11	7	High
CVE-2023-51782	linux - multiple products	An issue was discovered in the Linux kernel before 6.6.8. rose_ioctl in net/rose/af_rose.c has a use-after-free because of a rose_accept race condition.	2024-01-11	7	High
CVE-2024-21319	microsoft - multiple products	Microsoft Identity Denial of service vulnerability	2024-01-09	6.8	Medium
CVE-2024-20655	microsoft - multiple products	Microsoft Online Certificate Status Protocol (OCSP) Remote Code Execution Vulnerability	2024-01-09	6.6	Medium
CVE-2024-20666	microsoft - multiple products	BitLocker Security Feature Bypass Vulnerability	2024-01-09	6.6	Medium
CVE-2024-21736	sap - multiple products	SAP S/4HANA Finance for (Advanced Payment Management) - versions SAPSCORE 128, S4CORE 107, does not perform necessary authorization checks. A function import could be triggered allowing the attacker to create in-house bank accounts leading to low impact on the confidentiality of the application.	2024-01-09	6.5	Medium

CVE-2024-20660	microsoft - multiple products	Microsoft Message Queuing Information Disclosure Vulnerability	2024-01-09	6.5	Medium
CVE-2024-20663	microsoft - multiple products	Windows Message Queuing Client (MSMQC) Information Disclosure	2024-01-09	6.5	Medium
CVE-2024-20664	microsoft - multiple products	Microsoft Message Queuing Information Disclosure Vulnerability	2024-01-09	6.5	Medium
CVE-2024-20680	microsoft - multiple products	Windows Message Queuing Client (MSMQC) Information Disclosure	2024-01-09	6.5	Medium
CVE-2024-20690	microsoft - multiple products	Windows Nearby Sharing Spoofing Vulnerability	2024-01-09	6.5	Medium
CVE-2024-21314	microsoft - multiple products	Microsoft Message Queuing Information Disclosure Vulnerability	2024-01-09	6.5	Medium
CVE-2024-21320	microsoft - multiple products	Windows Themes Spoofing Vulnerability	2024-01-09	6.5	Medium
CVE-2023-37932	fortinet - multiple products	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability [CWE-22] in FortiVoiceEntreprise version 7.0.0 and before 6.4.7 allows an authenticated attacker to read arbitrary files from the system via sending crafted HTTP or HTTPS requests	2024-01-10	6.5	Medium
CVE-2023-37934	fortinet - fortipam	An allocation of resources without limits or throttling vulnerability [CWE-770] in FortiPAM 1.0 all versions allows an authenticated attacker to perform a denial of service attack via sending crafted HTTP or HTTPS requests in a high frequency.	2024-01-10	6.5	Medium
CVE-2023-40385	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14, Safari 17, iOS 17 and iPadOS 17. A remote attacker may be able to view leaked DNS queries with Private Relay turned on.	2024-01-10	6.5	Medium
CVE-2023-42862	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, iOS 16.4 and iPadOS 16.4, watchOS 9.4. Processing an image may result in disclosure of process memory.	2024-01-10	6.5	Medium
CVE-2023-42865	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3, tvOS 16.4, iOS 16.4 and iPadOS 16.4, watchOS 9.4. Processing an image may result in disclosure of process memory.	2024-01-10	6.5	Medium
CVE-2024-21982	netapp - multiple products	ONTAP versions 9.4 and higher are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information to unprivileged attackers when the object-store profiler command is being run by an administrative user.	2024-01-12	6.5	Medium

CVE-2023-36842	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in Juniper DHCP Daemon (jdhcpd) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause the jdhcpd to consume all the CPU cycles resulting in a Denial of Service (DoS).
		
		On Junos OS devices with forward-snooped-client configured, if an attacker sends a specific DHCP packet to a non-configured interface, this will cause an infinite loop. The DHCP process will have to be restarted to recover the service.
		
		This issue affects:
		
		Juniper Networks Junos OS
		
		* All versions earlier than 20.4R3-S9;
		* 21.2 versions earlier than 21.2R3-S7;
		* 21.3 versions earlier than 21.3R3-S5;
		* 21.4 versions earlier than 21.4R3-S5;
		* 22.1 versions earlier than 22.1R3-S4;
		* 22.2 versions earlier than 22.2R3-S3;
		* 22.3 versions earlier than 22.3R3-S2;
		* 22.4 versions earlier than 22.4R2-S2, 22.4R3;
		* 23.2 versions earlier than 23.2R2.
			2024-01-12	6.5	Medium

CVE-2024-21587	juniper - multiple products	An Improper Handling of Exceptional Conditions vulnerability in the broadband edge subscriber management daemon (bbe-smgd) of Juniper Networks Junos OS on MX Series allows an attacker directly connected to the vulnerable system who repeatedly flaps DHCP subscriber sessions to cause a slow memory leak, ultimately	2024-01-12	6.5	Medium

		leading to a Denial of Service (DoS). Memory can only be recovered by manually restarting bbe-smgd.
		
		This issue only occurs if BFD liveness detection for DHCP subscribers is enabled. Systems without BFD liveness detection enabled are not vulnerable to this issue.
		
		Indication of the issue can be observed by periodically executing the 'show system processes extensive' command, which will indicate an increase in memory allocation for bbe-smgd. A small amount of memory is leaked every time a DHCP subscriber logs in, which will become visible over time, ultimately leading to memory starvation.
		
		user@junos> show system processes extensive | match bbe-smgd
		13071 root 24 0 415M 201M select 0 0:41 7.28% bbe-smgd{bbe-smgd}
		13071 root 20 0 415M 201M select 1 0:04 0.00% bbe-smgd{bbe-smgd}
		...
		user@junos> show system processes extensive | match bbe-smgd
		13071 root 20 0 420M 208M select 0 4:33 0.10% bbe-smgd{bbe-smgd}
		13071 root 20 0 420M 208M select 0 0:12 0.00% bbe-smgd{bbe-smgd}
		...
		This issue affects Juniper Networks Junos OS on MX Series:
		
		* All versions earlier than 20.4R3-S9;
		* 21.2 versions earlier than 21.2R3-S7;
		* 21.3 versions earlier than 21.3R3-S5;
		* 21.4 versions earlier than 21.4R3-S5;
		* 22.1 versions earlier than 22.1R3-S4;
		* 22.2 versions earlier than 22.2R3-S3;
		* 22.3 versions earlier than 22.3R3-S2;
		* 22.4 versions earlier than 22.4R2-S2, 22.4R3;
		* 23.2 versions earlier than 23.2R1-S1, 23.2R2.			

CVE-2024-21599	juniper - multiple products	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). If an MX Series device receives PTP packets on an MPC3E that doesn't support PTP this causes a memory leak which will result in unpredictable behavior and ultimately in an MPC crash and restart. To monitor for this issue, please use the following FPC vty level commands: show heap shows an increase in "LAN buffer" utilization and show clksync ptp nbr-upd-info shows non-zero "Pending PFEs" counter. This issue affects Juniper Networks Junos OS on MX Series with MPC3E: * All versions earlier than 20.4R3-S3; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3; * 21.3 versions earlier than 21.3R2-S1, 21.3R3; * 21.4 versions earlier than 21.4R2; * 22.1 versions earlier than 22.1R2.	2024-01-12	6.5	Medium

CVE-2024-21600	juniper - multiple products	An Improper Neutralization of Equivalent Special Elements vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on PTX Series allows a unauthenticated, adjacent attacker to cause a Denial of Service (DoS). When MPLS packets are meant to be sent to a flexible tunnel interface (FTI) and if the FTI tunnel is down, these will hit the reject NH, due to which the packets get sent to the CPU and cause a host path wedge condition. This will cause the FPC to hang and requires a manual restart to recover. Please note that this issue specifically affects PTX1000, PTX3000, PTX5000 with FPC3, PTX10002-60C, and PTX10008/16 with LC110x. Other PTX Series devices and Line Cards (LC) are not affected. The following log message can be seen when the issue occurs: Cmerror Op Set: Host Loopback: HOST LOOPBACK WEDGE DETECTED IN PATH ID <id> (URI: /fpc/<fpc>/pfe/<pfe>/cm/<cm>/Host_Loopback/<cm>/HOST_LOOPBACK_MAKE_CMERROR_ID[<id>]) This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S8; * 21.1 versions earlier than 21.1R3-S4; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S5; * 22.1 versions earlier than 22.1R2-S2, 22.1R3; * 22.2 versions earlier than 22.2R2-S1, 22.2R3.	2024-01-12	6.5	Medium
CVE-2024-21603	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the kernel of Juniper Network Junos OS on MX Series allows a network based attacker with low privileges to cause a denial of service. If a scaled configuration for Source class usage (SCU) / destination class usage (DCU) (more than 10 route classes) is present and the SCU/DCU statistics are gathered by executing specific SNMP requests or CLI commands, a 'vmcore' for the RE kernel will be seen which leads to a device restart. Continued exploitation of this issue will lead to a sustained DoS. This issue only affects MX Series devices with MPC10, MPC11 or LC9600, and MX304. No other MX Series devices are affected. This issue affects Juniper Networks Junos OS: * All versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S6; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R2; * 22.3 versions earlier than 22.3R2.	2024-01-12	6.5	Medium
CVE-2024-21613	juniper - multiple products	A Missing Release of Memory after Effective Lifetime vulnerability in Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker to cause an rpd crash, leading to Denial of Service (DoS). On all Junos OS and Junos OS Evolved platforms, when traffic engineering is enabled for OSPF or ISIS, and a link flaps, a patroot memory leak is observed. This memory leak, over time, will lead to	2024-01-12	6.5	Medium

		an rpd crash and restart. The memory usage can be monitored using the below command. user@host> show task memory detail | match patroot This issue affects: Juniper Networks Junos OS * All versions earlier than 21.2R3-S3; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3; * 22.2 versions earlier than 22.2R3. Juniper Networks Junos OS Evolved * All versions earlier than 21.3R3-S5-EVO; * 21.4 versions earlier than 21.4R3-EVO; * 22.1 versions earlier than 22.1R3-EVO; * 22.2 versions earlier than 22.2R3-EVO.			
CVE-2024-21617	juniper - multiple products	An Incomplete Cleanup vulnerability in Nonstop active routing (NSR) component of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause memory leak leading to Denial of Service (DoS). On all Junos OS platforms, when NSR is enabled, a BGP flap will cause memory leak. A manual reboot of the system will restore the services. The memory usage can be monitored using the below commands. user@host> show chassis routing-engine no-forwarding user@host> show system memory | no-more This issue affects: Juniper Networks Junos OS * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S4; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions earlier than 22.1R3-S2; * 22.2 versions earlier than 22.2R3-S2; * 22.3 versions earlier than 22.3R2-S1, 22.3R3; * 22.4 versions earlier than 22.4R1-S2, 22.4R2. This issue does not affect Junos OS versions earlier than 20.4R3-S7.	2024-01-12	6.5	Medium
CVE-2024-20675	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2024-01-11	6.3	Medium
CVE-2024-21316	microsoft - multiple products	Windows Server Key Distribution Service Security Feature Bypass	2024-01-09	6.1	Medium
CVE-2024-0310	trellix - multiple products	A content-security-policy vulnerability in ENS Control browser extension prior to 10.7.0 Update 15 allows a remote attacker to alter the response header parameter setting to switch the content security policy into report-only mode, allowing an attacker to bypass the content-security-policy configuration.	2024-01-10	6.1	Medium
CVE-2024-21585	juniper - multiple products	An Improper Handling of Exceptional Conditions vulnerability in BGP session processing of Juniper Networks Junos OS and Junos	2024-01-12	5.9	Medium

		OS Evolved allows an unauthenticated network-based attacker, using specific timing outside the attacker's control, to flap BGP sessions and cause the routing protocol daemon (rpd) process to crash and restart, leading to a Denial of Service (DoS) condition. Continued BGP session flapping will create a sustained Denial of Service (DoS) condition.
		This issue only affects routers configured with non-stop routing (NSR) enabled. Graceful Restart (GR) helper mode, enabled by default, is also required for this issue to be exploitable.
		Note: NSR is not supported on the SRX Series and is therefore not affected by this vulnerability.
		When the BGP session flaps on the NSR-enabled router, the device enters GR-helper/LLGR-helper mode due to the peer having negotiated GR/LLGR-restarter capability and the backup BGP requests for replication of the GR/LLGR-helper session, master BGP schedules, and initiates replication of GR/LLGR stale routes to the backup BGP. In this state, if the BGP session with the BGP peer comes up again, unsolicited replication is initiated for the peer without cleaning up the ongoing GR/LLGR-helper mode replication. This parallel two instances of replication for the same peer leads to the assert if the BGP session flaps again.
		This issue affects:
		Juniper Networks Junos OS
		* All versions earlier than 20.4R3-S9;
		* 21.2 versions earlier than 21.2R3-S7;
		* 21.3 versions earlier than 21.3R3-S5;
		* 21.4 versions earlier than 21.4R3-S5;
		* 22.1 versions earlier than 22.1R3-S4;
		* 22.2 versions earlier than 22.2R3-S3;
		* 22.3 versions earlier than 22.3R3-S1;
		* 22.4 versions earlier than 22.4R2-S2, 22.4R3;
		* 23.2 versions earlier than 23.2R1-S1, 23.2R2.
		Juniper Networks Junos OS Evolved
		* All versions earlier than 21.3R3-S5-EVO;
		* 21.4 versions earlier than 21.4R3-S5-EVO;
		* 22.1 versions earlier than 22.1R3-S4-EVO;
		* 22.2 versions earlier than 22.2R3-S3-EVO;
		* 22.3 versions earlier than 22.3R3-S1-EVO;
		* 22.4 versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO;
		* 23.2 versions earlier than 23.2R1-S1-EVO, 23.2R2-EVO.			

CVE-2024-21601	juniper - multiple products	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the Flow-processing Daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (Dos). On SRX Series devices when two different threads try to simultaneously process a queue which is used for TCP events flowd will crash. One of these threads can not be triggered externally, so the exploitation of this race condition is outside the attackers direct control. Continued exploitation of this issue will lead to a sustained DoS. This issue affects Juniper Networks Junos OS: * 21.2 versions earlier than 21.2R3-S5; * 21.3 versions earlier than 21.3R3-S5;	2024-01-12	5.9	Medium

		* 21.4 versions earlier than 21.4R3-S4;
		* 22.1 versions earlier than 22.1R3-S3;
		* 22.2 versions earlier than 22.2R3-S1;
		* 22.3 versions earlier than 22.3R2-S2, 22.3R3;
		* 22.4 versions earlier than 22.4R2-S1, 22.4R3.
		This issue does not affect Juniper Networks Junos OS versions earlier than 21.2R1.			

CVE-2024-20692	microsoft - multiple products	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	2024-01-09	5.7	Medium
CVE-2024-21306	microsoft - multiple products	Microsoft Bluetooth Driver Spoofing Vulnerability	2024-01-09	5.7	Medium
CVE-2023-1032	linux - multiple products	The Linux kernel io_uring IORING_OP_SOCKET operation contained a double free in function __sys_socket_file() in file net/socket.c. This issue was introduced in da214a475f8bd1d3e9e7a19ddfeb4d1617551bab and fixed in 649c15c7691e9b13cbe9bf6c65c365350e056067.	2024-01-08	5.5	Medium
CVE-2023-51744	siemens - multiple products	A vulnerability has been identified in JT2Go (All versions < V14.3.0.6), Teamcenter Visualization V13.3 (All versions < V13.3.0.13), Teamcenter Visualization V14.1 (All versions < V14.1.0.12), Teamcenter Visualization V14.2 (All versions < V14.2.0.9), Teamcenter Visualization V14.3 (All versions < V14.3.0.6). The affected applications contain a null pointer dereference vulnerability while parsing specially crafted CGM files. An attacker could leverage this vulnerability to crash the application causing denial of service condition.	2024-01-09	5.5	Medium
CVE-2024-0340	linux - multiple products	A vulnerability was found in vhost_new_msg in drivers/vhost/vhost.c in the Linux kernel, which does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This issue can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.	2024-01-09	5.5	Medium
CVE-2024-20694	microsoft - multiple products	Windows CoreMessaging Information Disclosure Vulnerability	2024-01-09	5.5	Medium
CVE-2024-20699	microsoft - multiple products	Windows Hyper-V Denial of Service Vulnerability	2024-01-09	5.5	Medium
CVE-2024-21311	microsoft - multiple products	Windows Cryptographic Services Information Disclosure Vulnerability	2024-01-09	5.5	Medium
CVE-2024-20710	adobe - substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 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.	2024-01-10	5.5	Medium
CVE-2024-20711	adobe - substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 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.	2024-01-10	5.5	Medium
CVE-2024-20712	adobe - substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 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.	2024-01-10	5.5	Medium
CVE-2024-20713	adobe - substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 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.	2024-01-10	5.5	Medium
CVE-2024-20714	adobe - substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 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.	2024-01-10	5.5	Medium
CVE-2024-20715	adobe - substance_3d_stager	Adobe Substance 3D Stager versions 2.1.3 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	2024-01-10	5.5	Medium

		this issue requires user interaction in that a victim must open a malicious file.			
CVE-2022-32931	apple - macos	This issue was addressed with improved data protection. This issue is fixed in macOS Ventura 13. An app with root privileges may be able to access private information.	2024-01-10	5.5	Medium
CVE-2022-42816	apple - macos	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system.	2024-01-10	5.5	Medium
CVE-2022-46710	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. Location data may be shared via iCloud links even if Location metadata is disabled via the Share Sheet.	2024-01-10	5.5	Medium
CVE-2022-48504	apple - macos	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data.	2024-01-10	5.5	Medium
CVE-2022-48577	apple - macos	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Ventura 13. An app may be able to access user-sensitive data.	2024-01-10	5.5	Medium
CVE-2023-28185	apple - multiple products	An integer overflow was addressed through improved input validation. This issue is fixed in tvOS 16.4, macOS Big Sur 11.7.5, iOS 16.4 and iPadOS 16.4, watchOS 9.4, macOS Monterey 12.6.4, iOS 15.7.4 and iPadOS 15.7.4. An app may be able to cause a denial-of-service.	2024-01-10	5.5	Medium
CVE-2023-32424	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.4 and iPadOS 16.4, watchOS 9.4. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	2024-01-10	5.5	Medium
CVE-2023-38607	apple - macos	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14. An app may be able to modify Printer settings.	2024-01-10	5.5	Medium
CVE-2023-40411	apple - macos	This issue was addressed with improved data protection. This issue is fixed in macOS Sonoma 14. An app may be able to access user-sensitive data.	2024-01-10	5.5	Medium
CVE-2023-40430	apple - macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access removable volumes without user consent.	2024-01-10	5.5	Medium
CVE-2023-40433	apple - macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may bypass Gatekeeper checks.	2024-01-10	5.5	Medium
CVE-2023-40437	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to read sensitive location information.	2024-01-10	5.5	Medium
CVE-2023-40438	apple - multiple products	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14, iOS 16.7 and iPadOS 16.7. An app may be able to access edited photos saved to a temporary directory.	2024-01-10	5.5	Medium
CVE-2023-41069	apple - multiple products	This issue was addressed by improving Face ID anti-spoofing models. This issue is fixed in iOS 17 and iPadOS 17. A 3D model constructed to look like the enrolled user may authenticate via Face ID.	2024-01-10	5.5	Medium
CVE-2023-41987	apple - macos	This issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access sensitive user data.	2024-01-10	5.5	Medium
CVE-2023-41994	apple - macos	A logic issue was addressed with improved checks This issue is fixed in macOS Sonoma 14. A camera extension may be able to access the camera view from apps other than the app for which it was granted permission.	2024-01-10	5.5	Medium
CVE-2023-42829	apple - multiple products	The issue was addressed with additional restrictions on the observability of app states. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to access SSH passphrases.	2024-01-10	5.5	Medium
CVE-2023-42831	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to fingerprint the user.	2024-01-10	5.5	Medium
CVE-2023-42872	apple - multiple products	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app may be able to access sensitive user data.	2024-01-10	5.5	Medium
CVE-2023-42929	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may be able to access protected user data.	2024-01-10	5.5	Medium
CVE-2023-45173	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the NFS kernel extension to cause a denial of service. IBM X-Force ID: 267971.	2024-01-11	5.5	Medium
CVE-2023-45175	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 267973.	2024-01-11	5.5	Medium

CVE-2023-31001	ibm - multiple products	IBM Security Access Manager Container (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) temporarily stores sensitive information in files that could be accessed by a local user. IBM X-Force ID: 254653.	2024-01-11	5.5	Medium
CVE-2023-38267	ibm - multiple products	IBM Security Access Manager Appliance (IBM Security Verify Access Appliance 10.0.0.0 through 10.0.6.1 and IBM Security Verify Access Docker 10.0.6.1) could allow a local user to obtain sensitive configuration information. IBM X-Force ID: 260584.	2024-01-11	5.5	Medium
CVE-2023-45169	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the pmsvcs kernel extension to cause a denial of service. IBM X-Force ID: 267967.	2024-01-11	5.5	Medium
CVE-2023-45171	ibm - multiple products	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the kernel to cause a denial of service. IBM X-Force ID: 267969.	2024-01-11	5.5	Medium
CVE-2024-0443	linux - multiple products	A flaw was found in the blkgs destruction path in block/blk-cgroup.c in the Linux kernel, leading to a cgroup blkio memory leakage problem. When a cgroup is being destroyed, cgroup_rstat_flush() is only called at css_release_work_fn(), which is called when the blkcg reference count reaches 0. This circular dependency will prevent blkcg and some blkgs from being freed after they are made offline. This issue may allow an attacker with a local access to cause system instability, such as an out of memory error.	2024-01-12	5.5	Medium
CVE-2024-21594	juniper - multiple products	A Heap-based Buffer Overflow vulnerability in the Network Services Daemon (NSD) of Juniper Networks Junos OS allows authenticated, low privileged, local attacker to cause a Denial of Service (DoS). On an SRX 5000 Series device, when executing a specific command repeatedly, memory is corrupted, which leads to a Flow Processing Daemon (flowd) crash. The NSD process has to be restarted to restore services. If this issue occurs, it can be checked with the following command: user@host> request security policies check The following log message can also be observed: Error: policies are out of sync for PFE node<number>.fpc<number>.pic<number>. This issue affects: Juniper Networks Junos OS on SRX 5000 Series * All versions earlier than 20.4R3-S6; * 21.1 versions earlier than 21.1R3-S5; * 21.2 versions earlier than 21.2R3-S4; * 21.3 versions earlier than 21.3R3-S3; * 21.4 versions earlier than 21.4R3-S3; * 22.1 versions earlier than 22.1R3-S1; * 22.2 versions earlier than 22.2R3; * 22.3 versions earlier than 22.3R2.	2024-01-12	5.5	Medium
CVE-2022-48619	linux - linux_kernel	An issue was discovered in drivers/input/input.c in the Linux kernel before 5.17.10. An attacker can cause a denial of service (panic) because input_set_capability mishandles the situation in which an event code falls outside of a bitmap.	2024-01-12	5.5	Medium
CVE-2024-21734	sap - marketing	SAP Marketing (Contacts App) - version 160, allows an attacker with low privileges to trick a user to open malicious page which could lead to a very convincing phishing attack with low impact on confidentiality and integrity of the application.	2024-01-09	5.4	Medium
CVE-2024-21738	sap - multiple products	SAP NetWeaver ABAP Application Server and ABAP Platform do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. An attacker with low privileges can cause limited impact to confidentiality of the application data after successful exploitation.	2024-01-09	5.4	Medium
CVE-2023-5770	proofpoint - multiple products	Proofpoint Enterprise Protection contains a vulnerability in the email delivery agent that allows an unauthenticated attacker to inject improperly encoded HTML into the email body of a message through the email subject. The vulnerability is caused by inappropriate encoding when rewriting the email before	2024-01-09	5.4	Medium

		delivery.This issue affects Proofpoint Enterprise Protection: from 8.20.2 before patch 4809, from 8.20.0 before patch 4805, from 8.18.6 before patch 4804 and all other prior versions.			
CVE-2023-48783	fortinet - multiple products	An Authorization Bypass Through User-Controlled Key vulnerability [CWE-639] affecting PortiPortal version 7.2.1 and below, version 7.0.6 and below, version 6.0.14 and below, version 5.3.8 and below may allow a remote authenticated user with at least read-only permissions to access to other organization endpoints via crafted GET requests.	2024-01-10	5.4	Medium
CVE-2024-21313	microsoft - multiple products	Windows TCP/IP Information Disclosure Vulnerability	2024-01-09	5.3	Medium
CVE-2024-0333	google - chrome	Insufficient data validation in Extensions in Google Chrome prior to 120.0.6099.216 allowed an attacker in a privileged network position to install a malicious extension via a crafted HTML page. (Chromium security severity: High)	2024-01-10	5.3	Medium

CVE-2024-21596	juniper - multiple products	A Heap-based Buffer Overflow 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).
		If an attacker sends a specific BGP UPDATE message to the device, this will cause a memory overwrite and therefore an RPD crash and restart in the backup Routing Engine (RE). Continued receipt of these packets will cause a sustained Denial of Service (DoS) condition in the backup RE.
		The primary RE is not impacted by this issue and there is no impact on traffic.
		This issue only affects devices with NSR enabled.
		This issue requires an attacker to have an established BGP session to a system affected by the issue. This issue affects both eBGP and iBGP implementations.
		This issue affects:
		Juniper Networks Junos OS
		* All versions earlier than 20.4R3-S9;
		* 21.2 versions earlier than 21.2R3-S7;
		* 21.3 versions earlier than 21.3R3-S5;
		* 21.4 versions earlier than 21.4R3-S5;
		* 22.1 versions earlier than 22.1R3-S4;
		* 22.2 versions earlier than 22.2R3-S2;
		* 22.3 versions earlier than 22.3R3-S1;
		* 22.4 versions earlier than 22.4R2-S2, 22.4R3;
		* 23.1 versions earlier than 23.1R2;
		* 23.2 versions earlier than 23.2R1-S2, 23.2R2.
		Juniper Networks Junos OS Evolved
		* All versions earlier than 21.3R3-S5-EVO;
		* 21.4-EVO versions earlier than 21.4R3-S5-EVO;
		* 22.1-EVO versions earlier than 22.1R3-S4-EVO;
		* 22.2-EVO versions earlier than 22.2R3-S2-EVO;
		* 22.3-EVO versions later than 22.3R1-EVO;
		* 22.4-EVO versions earlier than 22.4R2-S2-EVO, 22.4R3-EVO;
		* 23.1-EVO versions earlier than 23.1R2-EVO;
		* 23.2-EVO versions earlier than 23.2R1-S2-EVO, 23.2R2-EVO.
			2024-01-12	5.3	Medium

CVE-2024-21607	juniper - multiple products	An Unsupported Feature in the UI vulnerability in Juniper Networks Junos OS on MX Series and EX9200 Series allows an unauthenticated, network-based attacker to cause partial impact to the integrity of the device. If the "tcp-reset" option is added to the "reject" action in an IPv6	2024-01-12	5.3	Medium

		filter which matches on "payload-protocol", packets are permitted instead of rejected. This happens because the payload-protocol match criteria is not supported in the kernel filter causing it to accept all packets without taking any other action. As a fix the payload-protocol match will be treated the same as a "next-header" match to avoid this filter bypass.
		This issue doesn't affect IPv4 firewall filters.
		This issue affects Juniper Networks Junos OS on MX Series and EX9200 Series:
		* All versions earlier than 20.4R3-S7;
		* 21.1 versions earlier than 21.1R3-S5;
		* 21.2 versions earlier than 21.2R3-S5;
		* 21.3 versions earlier than 21.3R3-S4;
		* 21.4 versions earlier than 21.4R3-S4;
		* 22.1 versions earlier than 22.1R3-S2;
		* 22.2 versions earlier than 22.2R3-S2;
		* 22.3 versions earlier than 22.3R2-S2, 22.3R3;
		* 22.4 versions earlier than 22.4R1-S2, 22.4R2-S2, 22.4R3.			

CVE-2024-21337	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-11	5.2	Medium
CVE-2024-20662	microsoft - multiple products	Windows Online Certificate Status Protocol (OCSP) Information Disclosure Vulnerability	2024-01-09	4.9	Medium
CVE-2023-42941	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 17.2 and iPadOS 17.2. An attacker in a privileged network position may be able to perform a denial-of-service attack using crafted Bluetooth packets.	2024-01-10	4.8	Medium
CVE-2024-20691	microsoft - multiple products	Windows Themes Information Disclosure Vulnerability	2024-01-09	4.7	Medium
CVE-2022-32919	apple - multiple products	The issue was addressed with improved UI handling. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. Visiting a website that frames malicious content may lead to UI spoofing.	2024-01-10	4.7	Medium
CVE-2024-21305	microsoft - multiple products	Hypervisor-Protected Code Integrity (HVCI) Security Feature Bypass Vulnerability	2024-01-09	4.4	Medium
CVE-2023-42934	apple - multiple products	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14, iOS 17 and iPadOS 17. An app with root privileges may be able to access private information.	2024-01-10	4.2	Medium
CVE-2022-42839	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. An app may be able to read sensitive location information.	2024-01-10	3.3	Low
CVE-2023-28197	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.3, macOS Big Sur 11.7.5, macOS Monterey 12.6.4. An app may be able to access user-sensitive data.	2024-01-10	3.3	Low
CVE-2023-38612	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.7, iOS 16.7 and iPadOS 16.7, iOS 17 and iPadOS 17, macOS Sonoma 14, macOS Ventura 13.6. An app may be able to access protected user data.	2024-01-10	3.3	Low
CVE-2023-40383	apple - macos	A path handling issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3. An app may be able to access user-sensitive data.	2024-01-10	3.3	Low
CVE-2023-40394	apple - multiple products	The issue was addressed with improved validation of environment variables. This issue is fixed in iOS 16.6 and iPadOS 16.6. An app may be able to access sensitive user data.	2024-01-10	3.3	Low
CVE-2023-40439	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to read sensitive location information.	2024-01-10	3.3	Low
CVE-2023-42830	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3, iOS 16.4 and iPadOS 16.4. An app may be able to read sensitive location information.	2024-01-10	3.3	Low
CVE-2023-49619	apache - answer	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Answer. This issue affects Apache Answer: through 1.2.0. Under normal circumstances, a user can only bookmark a question	2024-01-10	3.1	Low

		once, and will only increase the number of questions bookmarked once. However, repeat submissions through the script can increase the number of collection of the question many times. Users are recommended to upgrade to version [1.2.1], which fixes the issue.			
CVE-2023-40529	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 17 and iPadOS 17. A person with physical access to a device may be able to use VoiceOver to access private calendar information.	2024-01-10	2.4	Low
CVE-2024-0230	apple - magic_keyboard_firmware	A session management issue was addressed with improved checks. This issue is fixed in Magic Keyboard Firmware Update 2.0.6. An attacker with physical access to the accessory may be able to extract its Bluetooth pairing key and monitor Bluetooth traffic.	2024-01-12	2.4	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.