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 ٢١ يناير إلى ٢٧ يناير. 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 21st of January to 27th 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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-20253	cisco - multiple products	A vulnerability in multiple Cisco Unified Communications and Contact Center Solutions products could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to the improper processing of user-provided data that is being read into memory. An attacker could exploit this vulnerability by sending a crafted message to a listening port of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the web services user. With access to the underlying operating system, the attacker could also establish root access on the affected device.	2024-01-26	10	Critical
CVE-2024-0808	google - chrome	Integer underflow in WebUI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a malicious file. (Chromium security severity: High)	2024-01-24	9.8	Critical
CVE-2023-40547	redhat - shim	A remote code execution vulnerability was found in Shim. The Shim boot support trusts attacker-controlled values when parsing an HTTP response. This flaw allows an attacker to craft a specific malicious HTTP request, leading to a completely controlled out-of-bounds write primitive and complete system compromise.	2024-01-25	9.8	Critical
CVE-2024-23619	ibm - merge_efilm_workstation	A hardcoded credential vulnerability exists in IBM Merge Healthcare eFilm Workstation. A remote, unauthenticated attacker can exploit this vulnerability to achieve information disclosure or remote code execution.	2024-01-26	9.8	Critical
CVE-2024-23621	ibm - merge_efilm_workstation	A buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution.	2024-01-26	9.8	Critical
CVE-2024-23622	ibm - merge_efilm_workstation	A stack-based buffer overflow exists in IBM Merge Healthcare eFilm Workstation license server. A remote, unauthenticated attacker can exploit this vulnerability to achieve remote code execution with SYSTEM privileges.	2024-01-26	9.8	Critical
CVE-2024-21326	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-26	9.6	Critical
CVE-2024-23209	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3. Processing web content may lead to arbitrary code execution.	2024-01-23	8.8	High
CVE-2024-23213	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. Processing web content may lead to arbitrary code execution.	2024-01-23	8.8	High
CVE-2024-23214	apple - multiple products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, iOS 17.3 and iPadOS 17.3. Processing maliciously crafted web content may lead to arbitrary code execution.	2024-01-23	8.8	High
CVE-2024-23222	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. Processing maliciously	2024-01-23	8.8	High

		crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited.			
CVE-2024-0745	mozilla - firefox	The WebAudio `OscillatorNode` object was susceptible to a stack buffer overflow. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 122.	2024-01-23	8.8	High
CVE-2024-0750	mozilla - multiple products	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	8.8	High
CVE-2024-0751	mozilla - multiple products	A malicious devtools extension could have been used to escalate privileges. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	8.8	High
CVE-2024-0755	mozilla - multiple products	Memory safety bugs present in Firefox 121, Firefox ESR 115.6, and Thunderbird 115.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	8.8	High
CVE-2023-52324	trendmicro - apex_central	An unrestricted file upload vulnerability in Trend Micro Apex Central could allow a remote attacker to create arbitrary files on affected installations. Please note: although authentication is required to exploit this vulnerability, this vulnerability could be exploited when the attacker has any valid set of credentials. Also, this vulnerability could be potentially used in combination with another vulnerability to execute arbitrary code.	2024-01-23	8.8	High
CVE-2024-0806	google - chrome	Use after free in Passwords in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)	2024-01-24	8.8	High
CVE-2024-0807	google - chrome	Use after free in Web Audio in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-24	8.8	High
CVE-2024-0812	google - chrome	Inappropriate implementation in Accessibility in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2024-01-24	8.8	High
CVE-2024-0813	google - chrome	Use after free in Reading Mode in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interaction. (Chromium security severity: Medium)	2024-01-24	8.8	High
CVE-2024-23898	jenkins - multiple products	Jenkins 2.217 through 2.441 (both inclusive), LTS 2.222.1 through 2.426.2 (both inclusive) does not perform origin validation of requests made through the CLI WebSocket endpoint, resulting in a cross-site WebSocket hijacking (CSWSH) vulnerability, allowing attackers to execute CLI commands on the Jenkins controller.	2024-01-24	8.8	High
CVE-2024-21385	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2024-01-26	8.3	High
CVE-2023-51833	trendnet - tew-411brpplus_firmware	A command injection issue in TRENDnet TEW-411BRPplus v.2.07_eu that allows a local attacker to execute arbitrary code via the data1 parameter in the debug.cgi page.	2024-01-25	8.1	High
CVE-2023-42881	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.2. Processing a file may lead to unexpected app termination or arbitrary code execution.	2024-01-23	7.8	High
CVE-2024-23208	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to execute arbitrary code with kernel privileges.	2024-01-23	7.8	High
CVE-2024-23212	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to execute arbitrary code with kernel privileges.	2024-01-23	7.8	High
CVE-2023-51042	linux - linux_kernel	In the Linux kernel before 6.4.12, amdgpu_cs_wait_all_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c has a fence use-after-free.	2024-01-23	7.8	High
CVE-2024-22705	linux - multiple products	An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strndup_from_utf16 out-of-bounds access because the relationship between Name data and CreateContexts data is mishandled.	2024-01-23	7.8	High
CVE-2023-50274	hp - oneview	HPE OneView may allow command injection with local privilege escalation.	2024-01-23	7.8	High
CVE-2023-47192	trendmicro - multiple products	An agent link vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected	2024-01-23	7.8	High

		installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.			
CVE-2023-47193	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47194.	2024-01-23	7.8	High
CVE-2023-47194	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47195.	2024-01-23	7.8	High
CVE-2023-47195	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47196.	2024-01-23	7.8	High
CVE-2023-47196	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47197.	2024-01-23	7.8	High
CVE-2023-47197	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47198.	2024-01-23	7.8	High
CVE-2023-47198	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations.	2024-01-23	7.8	High

		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47199.			
CVE-2023-47199	trendmicro - multiple products	An origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47193.	2024-01-23	7.8	High
CVE-2023-47200	trendmicro - multiple products	A plug-in manager origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47201.	2024-01-23	7.8	High
CVE-2023-47201	trendmicro - multiple products	A plug-in manager origin validation vulnerability in the Trend Micro Apex One security agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to, but not identical to, CVE-2023-47200.	2024-01-23	7.8	High
CVE-2023-47202	trendmicro - multiple products	A local file inclusion vulnerability on the Trend Micro Apex One management server could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2023-52090	trendmicro - multiple products	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2023-52091	trendmicro - multiple products	An anti-spyware engine link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High

CVE-2023-52092	trendmicro - multiple products	A security agent link following vulnerability in Trend Micro Apex One could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2023-52093	trendmicro - multiple products	An exposed dangerous function vulnerability in the Trend Micro Apex One agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2023-52094	trendmicro - multiple products	An updater link following vulnerability in the Trend Micro Apex One agent could allow a local attacker to abuse the updater to delete an arbitrary folder, leading for a local privilege escalation on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2023-52337	trendmicro - multiple products	An improper access control vulnerability in Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload Security Agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2023-52338	trendmicro - multiple products	A link following vulnerability in the Trend Micro Deep Security 20.0 and Trend Micro Cloud One - Endpoint and Workload Security Agent could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.8	High
CVE-2024-23307	linux - linux_kernel	Integer Overflow or Wraparound vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (md, raid, raid5 modules) allows Forced Integer Overflow.	2024-01-25	7.8	High
CVE-2024-23620	ibm - merge_efilm_workstation	An improper privilege management vulnerability exists in IBM Merge Healthcare eFilm Workstation. A local, authenticated attacker can exploit this vulnerability to escalate privileges to SYSTEM.	2024-01-26	7.8	High
CVE-2024-22545	trendnet - tew-824dru_firmware	An issue was discovered in TRENDnet TEW-824DRU version 1.04b01, allows local unauthenticated attackers to execute arbitrary code via the system.ntp.server parameter in the sub_420AE0() function.	2024-01-26	7.8	High
CVE-2024-22233	vmware - multiple products	In Spring Framework versions 6.0.15 and 6.1.2, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Specifically, an application is vulnerable when all of the following are true: * the application uses Spring MVC * Spring Security 6.1.6+ or 6.2.1+ is on the classpath Typically, Spring Boot applications need the org.springframework.boot:spring-boot-starter-web and org.springframework.boot:spring-boot-starter-security dependencies to meet all conditions.	2024-01-22	7.5	High
CVE-2023-45193	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 federated server is vulnerable to a denial of service when a specially crafted cursor is used. IBM X-Force ID: 268759.	2024-01-22	7.5	High

CVE-2024-0605	mozilla - firefox_focus	Using a javascript: URI with a setTimeout race condition, an attacker can execute unauthorized scripts on top origin sites in urlbar. This bypasses security measures, potentially leading to arbitrary code execution or unauthorized actions within the user's loaded webpage. This vulnerability affects Focus for iOS < 122.	2024-01-22	7.5	High
CVE-2023-47152	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an insecure cryptographic algorithm and to information disclosure in stack trace under exceptional conditions. IBM X-Force ID: 270730.	2024-01-22	7.5	High
CVE-2024-23203	apple - multiple products	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user.	2024-01-23	7.5	High
CVE-2024-23204	apple - multiple products	The issue was addressed with additional permissions checks. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. A shortcut may be able to use sensitive data with certain actions without prompting the user.	2024-01-23	7.5	High
CVE-2023-39197	linux - linux_kernel	An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. This flaw allows a remote user to disclose sensitive information via the DCCP protocol.	2024-01-23	7.5	High
CVE-2024-0743	mozilla - firefox	An unchecked return value in TLS handshake code could have caused a potentially exploitable crash. This vulnerability affects Firefox < 122.	2024-01-23	7.5	High
CVE-2024-0744	mozilla - firefox	In some circumstances, JIT compiled code could have dereferenced a wild pointer value. This could have led to an exploitable crash. This vulnerability affects Firefox < 122.	2024-01-23	7.5	High
CVE-2023-50275	hp - oneview	HPE OneView may allow clusterService Authentication Bypass resulting in denial of service.	2024-01-23	7.5	High
CVE-2023-52325	trendmicro - apex_central	A local file inclusion vulnerability in one of Trend Micro Apex Central's widgets could allow a remote attacker to execute arbitrary code on affected installations. Please note: this vulnerability must be used in conjunction with another one to exploit an affected system. In addition, an attacker must first obtain a valid set of credentials on target system in order to exploit this vulnerability.	2024-01-23	7.5	High
CVE-2024-0804	google - chrome	Insufficient policy enforcement in iOS Security UI in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2024-01-24	7.5	High
CVE-2023-50943	apache - airflow	Apache Airflow, versions before 2.8.1, have a vulnerability that allows a potential attacker to poison the XCom data by bypassing the protection of "enable_xcom_pickling=False" configuration setting resulting in poisoned data after XCom deserialization. This vulnerability is considered low since it requires a DAG author to exploit it. Users are recommended to upgrade to version 2.8.1 or later, which fixes this issue.	2024-01-24	7.5	High
CVE-2024-23897	jenkins - multiple products	Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.	2024-01-24	7.5	High
CVE-2024-23904	jenkins - log_command	Jenkins Log Command Plugin 1.0.2 and earlier does not disable a feature of its command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read content from arbitrary files on the Jenkins controller file system.	2024-01-24	7.5	High
CVE-2024-21619	juniper - multiple products	A Missing Authentication for Critical Function vulnerability combined with a Generation of Error Message Containing Sensitive Information vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an unauthenticated, network-based attacker to access sensitive system information. When a user logs in, a temporary file which contains the configuration of the device (as visible to that user) is created in the /cache folder. An unauthenticated attacker can then attempt to access such a file by sending a specific request to the device trying to guess the name of such a file. Successful exploitation will reveal configuration information. This issue affects Juniper Networks Junos OS on SRX Series and EX 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-S6;	2024-01-25	7.5	High

		* 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.			
CVE-2024-0918	trendnet - tew-800mb_firmware	A vulnerability was found in TRENDnet TEW-800MB 1.0.1.0 and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument DeviceURL leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-252122 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.2	High
CVE-2024-0919	trendnet - tew-815dap_firmware	A vulnerability was found in TRENDnet TEW-815DAP 1.0.2.0. It has been classified as critical. This affects the function do_setNTP of the component POST Request Handler. The manipulation of the argument NtpDstStart/NtpDstEnd leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-252123. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.2	High
CVE-2024-0920	trendnet - tew-822dre_firmware	A vulnerability was found in TRENDnet TEW-822DRE 1.03B02. It has been declared as critical. This vulnerability affects unknown code of the file /admin_ping.htm of the component POST Request Handler. The manipulation of the argument ipv4_ping/ipv6_ping leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-252124. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2024-01-26	7.2	High
CVE-2024-0775	linux - multiple products	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential failure, leading to a use-after-free.	2024-01-22	7.1	High
CVE-2023-52331	trendmicro - apex_central	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2024-01-23	7.1	High
CVE-2023-44281	dell - pair	Dell Pair Installer version prior to 1.2.1 contains an elevation of privilege vulnerability. A low privilege user with local access to the system could potentially exploit this vulnerability to delete arbitrary files and result in Denial of Service.	2024-01-24	7.1	High
CVE-2023-6531	linux - multiple products	A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on.	2024-01-21	7	High
CVE-2023-51043	linux - linux_kernel	In the Linux kernel before 6.4.5, drivers/gpu/drm/drm_atomic.c has a use-after-free during a race condition between a nonblocking atomic commit and a driver unload.	2024-01-23	7	High
CVE-2023-47746	ibm - multiple products	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272644.	2024-01-22	6.5	Medium
CVE-2023-50308	ibm - db2	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM X-Force ID: 273393.	2024-01-22	6.5	Medium
CVE-2023-27859	ibm - multiple products	IBM Db2 10.1, 10.5, and 11.1 could allow a remote user to execute arbitrary code caused by installing like named jar files across multiple databases. A user could exploit this by installing a malicious jar file that overwrites the existing like named jar file in another database. IBM X-Force ID: 249205.	2024-01-22	6.5	Medium
CVE-2023-47158	ibm - multiple products	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270750.	2024-01-22	6.5	Medium
CVE-2023-47747	ibm - multiple products	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated user with	2024-01-22	6.5	Medium

		CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 272646.			
CVE-2023-47141	ibm - db2	IIBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user with CONNECT privileges to cause a denial of service using a specially crafted query. IBM X-Force ID: 270264.	2024-01-22	6.5	Medium
CVE-2024-23206	apple - multiple products	An access issue was addressed with improved access restrictions. This issue is fixed in watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A maliciously crafted webpage may be able to fingerprint the user.	2024-01-23	6.5	Medium
CVE-2024-0741	mozilla - multiple products	An out of bounds write in ANGLE could have allowed an attacker to corrupt memory leading to a potentially exploitable crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	6.5	Medium
CVE-2024-0746	mozilla - multiple products	A Linux user opening the print preview dialog could have caused the browser to crash. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	6.5	Medium
CVE-2024-0747	mozilla - multiple products	When a parent page loaded a child in an iframe with `unsafe-inline`, the parent Content Security Policy could have overridden the child Content Security Policy. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	6.5	Medium
CVE-2024-0752	mozilla - firefox	A use-after-free crash could have occurred on macOS if a Firefox update were being applied on a very busy system. This could have resulted in an exploitable crash. This vulnerability affects Firefox < 122.	2024-01-23	6.5	Medium
CVE-2024-0753	mozilla - multiple products	In specific HSTS configurations an attacker could have bypassed HSTS on a subdomain. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	6.5	Medium
CVE-2024-0754	mozilla - firefox	Some WASM source files could have caused a crash when loaded in devtools. This vulnerability affects Firefox < 122.	2024-01-23	6.5	Medium
CVE-2024-0814	google - chrome	Incorrect security UI in Payments in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to potentially spoof security UI via a crafted HTML page. (Chromium security severity: Medium)	2024-01-24	6.5	Medium
CVE-2023-50944	apache - airflow	Apache Airflow, versions before 2.8.1, have a vulnerability that allows an authenticated user to access the source code of a DAG to which they don't have access. This vulnerability is considered low since it requires an authenticated user to exploit it. Users are recommended to upgrade to version 2.8.1, which fixes this issue.	2024-01-24	6.5	Medium
CVE-2023-51702	apache - multiple products	Since version 5.2.0, when using deferrable mode with the path of a Kubernetes configuration file for authentication, the Airflow worker serializes this configuration file as a dictionary and sends it to the triggerer by storing it in metadata without any encryption. Additionally, if used with an Airflow version between 2.3.0 and 2.6.0, the configuration dictionary will be logged as plain text in the triggerer service without masking. This allows anyone with access to the metadata or triggerer log to obtain the configuration file and use it to access the Kubernetes cluster. This behavior was changed in version 7.0.0, which stopped serializing the file contents and started providing the file path instead to read the contents into the trigger. Users are recommended to upgrade to version 7.0.0, which fixes this issue.	2024-01-24	6.5	Medium
CVE-2024-23899	jenkins - git_server	Jenkins Git server Plugin 99.va_0826a_b_cdfa_d and earlier does not disable a feature of its command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing attackers with Overall/Read permission to read content from arbitrary files on the Jenkins controller file system.	2024-01-24	6.5	Medium
CVE-2024-23901	jenkins - github_branch_source	Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier unconditionally discovers projects that are shared with the configured owner group, allowing attackers to configure and share a project, resulting in a crafted Pipeline being built by Jenkins during the next scan of the group.	2024-01-24	6.5	Medium
CVE-2024-22432	dell - networker	Networker 19.9 and all prior versions contains a Plain-text Password stored in temporary config file during backup duration in NMDA MySQL Database backups. User has low privilege access to Networker Client system could potentially exploit this vulnerability, leading to the disclosure of configured MySQL Database user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application Database with privileges of the compromised account.	2024-01-25	6.5	Medium
CVE-2023-41474	ivanti - avalanche	Directory Traversal vulnerability in Ivanti Avalanche 6.3.4.153 allows a remote authenticated attacker to obtain sensitive information via the javax.faces.resource component.	2024-01-25	6.5	Medium
CVE-2023-42887	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.6.4, macOS Sonoma 14.2. An app may be able to read arbitrary files.	2024-01-23	6.3	Medium

CVE-2024-23219	apple - multiple products	The issue was addressed with improved authentication. This issue is fixed in iOS 17.3 and iPadOS 17.3. Stolen Device Protection may be unexpectedly disabled.	2024-01-23	6.2	Medium
CVE-2024-23223	apple - multiple products	A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access sensitive user data.	2024-01-23	6.2	Medium
CVE-2024-0606	mozilla - firefox_focus	An attacker could execute unauthorized script on a legitimate site through UXSS using window.open() by opening a javascript URI leading to unauthorized actions within the user's loaded webpage. This vulnerability affects Focus for iOS < 122.	2024-01-22	6.1	Medium
CVE-2023-41176	trendmicro - mobile_security	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41177.	2024-01-23	6.1	Medium
CVE-2023-41177	trendmicro - mobile_security	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41178.	2024-01-23	6.1	Medium
CVE-2023-41178	trendmicro - mobile_security	Reflected cross-site scripting (XSS) vulnerabilities in Trend Micro Mobile Security (Enterprise) could allow an exploit against an authenticated victim that visits a malicious link provided by an attacker. Please note, this vulnerability is similar to, but not identical to, CVE-2023-41176.	2024-01-23	6.1	Medium
CVE-2023-52326	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52327.	2024-01-23	6.1	Medium
CVE-2023-52327	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52328.	2024-01-23	6.1	Medium
CVE-2023-52328	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52329.	2024-01-23	6.1	Medium
CVE-2023-52329	trendmicro - apex_central	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote code execution on affected servers. Please note this vulnerability is similar, but not identical to CVE-2023-52326.	2024-01-23	6.1	Medium
CVE-2023-52330	trendmicro - multiple products	A cross-site scripting vulnerability in Trend Micro Apex Central could allow a remote attacker to execute arbitrary code on affected installations of Trend Micro Apex Central.	2024-01-23	6.1	Medium

		Please note: user interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.			
CVE-2024-21620	juniper - multiple products	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives. This issue affects Juniper Networks Junos OS on SRX Series and EX Series: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S8; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S2; * 22.4 versions earlier than 22.4R3-S1; * 23.2 versions earlier than 23.2R2; * 23.4 versions earlier than 23.4R2.	2024-01-25	6.1	Medium
CVE-2023-6291	redhat - multiple products	A flaw was found in the redirect_uri validation logic in Keycloak. This issue may allow a bypass of otherwise explicitly allowed hosts. A successful attack may lead to an access token being stolen, making it possible for the attacker to impersonate other users.	2024-01-26	6.1	Medium
CVE-2024-23218	apple - multiple products	A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key.	2024-01-23	5.9	Medium
CVE-2023-40528	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 17, watchOS 10, macOS Sonoma 14, iOS 17 and iPadOS 17, macOS Ventura 13.6.4. An app may be able to bypass Privacy preferences.	2024-01-23	5.5	Medium
CVE-2023-42888	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. Processing a maliciously crafted image may result in disclosure of process memory.	2024-01-23	5.5	Medium
CVE-2023-42935	apple - multiple products	An authentication issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.6.4. A local attacker may be able to view the previous logged in user's desktop from the fast user switching screen.	2024-01-23	5.5	Medium
CVE-2023-42937	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 16.7.5 and iPadOS 16.7.5, watchOS 10.2, macOS Ventura 13.6.4, macOS Sonoma 14.2, macOS Monterey 12.7.3, iOS 17.2 and iPadOS 17.2. An app may be able to access sensitive user data.	2024-01-23	5.5	Medium
CVE-2024-23207	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3. An app may be able to access sensitive user data.	2024-01-23	5.5	Medium
CVE-2024-23215	apple - multiple products	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to access user-sensitive data.	2024-01-23	5.5	Medium
CVE-2024-23224	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.3, macOS Ventura 13.6.4. An app may be able to access sensitive user data.	2024-01-23	5.5	Medium
CVE-2024-23848	linux - linux_kernel	In the Linux kernel through 6.7.1, there is a use-after-free in cec_queue_msg_fh, related to drivers/media/cec/core/cec-adap.c and drivers/media/cec/core/cec-api.c.	2024-01-23	5.5	Medium
CVE-2024-23849	linux - linux_kernel	In rds_recv_track_latency in net/rds/af_rds.c in the Linux kernel through 6.7.1, there is an off-by-one error for an RDS_MSG_RX_DGRAM_TRACE_MAX comparison, resulting in out-of-bounds access.	2024-01-23	5.5	Medium
CVE-2024-23850	linux - linux_kernel	In btrfs_get_root_ref in fs/btrfs/disk-io.c in the Linux kernel through 6.7.1, there can be an assertion failure and crash because a subvolume can be read out too soon after its root item is inserted upon subvolume creation.	2024-01-23	5.5	Medium
CVE-2024-23851	linux - linux_kernel	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1 can attempt to allocate more than INT_MAX bytes, and	2024-01-23	5.5	Medium

		crash, because of a missing param_kernel->data_size check. This is related to ctl_ioctl.			
CVE-2023-46343	linux - linux_kernel	In the Linux kernel before 6.5.9, there is a NULL pointer dereference in send_acknowledge in net/nfc/nci/spi.c.	2024-01-23	5.5	Medium
CVE-2023-6573	hp - oneview	HPE OneView may have a missing passphrase during restore.	2024-01-23	5.5	Medium
CVE-2024-22099	linux - linux_kernel	NULL Pointer Dereference vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (net, bluetooth modules) allows Overflow Buffers. This vulnerability is associated with program files /net/bluetooth/rfcomm/core.C. This issue affects Linux kernel: v2.6.12-rc2.	2024-01-25	5.5	Medium
CVE-2024-0727	openssl - multiple products	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.	2024-01-26	5.5	Medium

CVE-2023-49657	apache - superset	A stored cross-site scripting (XSS) vulnerability exists in Apache Superset before 3.0.3. An authenticated attacker with create/update permissions on charts or dashboards could store a script or add a specific HTML snippet that would act as a stored XSS.
		
		For 2.X versions, users should change their config to include:
		
		TALISMAN_CONFIG = {
		"content_security_policy": {
		"base-uri": ["'self'"],
		"default-src": ["'self'"],
		"img-src": ["'self'", "blob:", "data:"],
		"worker-src": ["'self'", "blob:"],
		"connect-src": [
		"'self'",
		" https://api.mapbox.com" https://api.mapbox.com" ;,
		" https://events.mapbox.com" https://events.mapbox.com"
		;,
		],
		"object-src": "'none'",
		"style-src": [
		"'self'",
		"'unsafe-inline'",
		],
		"script-src": ["'self'", "'strict-dynamic'"],
		},
		"content_security_policy_nonce_in": ["script-src"],
		"force_https": False,
		"session_cookie_secure": False,
		}
			2024-01-23	5.4	Medium

CVE-2023-38624	trendmicro - apex_central	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly.	2024-01-23	5.4	Medium

		Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38625 through CVE-2023-38627.			
CVE-2023-38625	trendmicro - apex_central	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38624.	2024-01-23	5.4	Medium
CVE-2023-38626	trendmicro - apex_central	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38625.	2024-01-23	5.4	Medium
CVE-2023-38627	trendmicro - apex_central	A post-authenticated server-side request forgery (SSRF) vulnerability in Trend Micro Apex Central 2019 (lower than build 6481) could allow an attacker to interact with internal or local services directly. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-38626.	2024-01-23	5.4	Medium
CVE-2024-0854	synology - diskstation_manager	URL redirection to untrusted site ('Open Redirect') vulnerability in file access component in Synology DiskStation Manager (DSM) before 7.2.1-69057-2 allows remote authenticated users to conduct phishing attacks via unspecified vectors.	2024-01-24	5.4	Medium
CVE-2024-23905	jenkins - red_hat_dependency_analytics	Jenkins Red Hat Dependency Analytics Plugin 0.7.1 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	2024-01-24	5.4	Medium
CVE-2024-23903	jenkins - github_branch_source	Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2024-01-24	5.3	Medium
CVE-2024-21387	microsoft - multiple products	Microsoft Edge for Android Spoofing Vulnerability	2024-01-26	5.3	Medium
CVE-2021-43584	nagios - nagios_cross_platform_agent	DOM-based Cross Site Scripting (XSS vulnerability in 'Tail Event Logs' functionality in Nagios Nagios Cross-Platform Agent (NCPA) before 2.4.0 allows attackers to run arbitrary code via the name element when filtering for a log.	2024-01-24	4.8	Medium
CVE-2024-20305	cisco - unity_connection	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-01-26	4.8	Medium

CVE-2024-0742	mozilla - multiple products	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an incorrect timestamp used to prevent input after page load. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	4.3	Medium
CVE-2024-0748	mozilla - firefox	A compromised content process could have updated the document URI. This could have allowed an attacker to set an arbitrary URI in the address bar or history. This vulnerability affects Firefox < 122.	2024-01-23	4.3	Medium
CVE-2024-0749	mozilla - multiple products	A phishing site could have repurposed an `about:` dialog to show phishing content with an incorrect origin in the address bar. This vulnerability affects Firefox < 122, Firefox ESR < 115.7, and Thunderbird < 115.7.	2024-01-23	4.3	Medium
CVE-2024-0805	google - chrome	Inappropriate implementation in Downloads in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium)	2024-01-24	4.3	Medium
CVE-2024-0809	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 121.0.6167.85 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Low)	2024-01-24	4.3	Medium
CVE-2024-0810	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium)	2024-01-24	4.3	Medium
CVE-2024-0811	google - chrome	Inappropriate implementation in Extensions API in Google Chrome prior to 121.0.6167.85 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low)	2024-01-24	4.3	Medium
CVE-2024-22229	dell - multiple products	Dell Unity, versions prior to 5.4, contain a vulnerability whereby log messages can be spoofed by an authenticated attacker. An attacker could exploit this vulnerability to forge log entries, create false alarms, and inject malicious content into logs that compromise logs integrity. A malicious attacker could also prevent the product from logging information while malicious actions are performed or implicate an arbitrary user for malicious activities.	2024-01-24	4.3	Medium
CVE-2024-23900	jenkins - matrix_project	Jenkins Matrix Project Plugin 822.v01b_8c85d16d2 and earlier does not sanitize user-defined axis names of multi-configuration projects, allowing attackers with Item/Configure permission to create or replace any config.xml files on the Jenkins controller file system with content not controllable by the attackers.	2024-01-24	4.3	Medium
CVE-2024-23902	jenkins - github_branch_source	A cross-site request forgery (CSRF) vulnerability in Jenkins GitLab Branch Source Plugin 684.vea_fa_7c1e2fe3 and earlier allows attackers to connect to an attacker-specified URL.	2024-01-24	4.3	Medium
CVE-2024-21382	microsoft - edge_chromium	Microsoft Edge for Android Information Disclosure Vulnerability	2024-01-26	4.3	Medium
CVE-2024-23210	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iOS 17.3 and iPadOS 17.3. An app may be able to view a user's phone number in system logs.	2024-01-23	3.3	Low
CVE-2024-23211	apple - multiple products	A privacy issue was addressed with improved handling of user preferences. This issue is fixed in watchOS 10.3, iOS 17.3 and iPadOS 17.3, macOS Sonoma 14.3, iOS 16.7.5 and iPadOS 16.7.5, Safari 17.3. A user's private browsing activity may be visible in Settings.	2024-01-23	3.3	Low
CVE-2024-23217	apple - multiple products	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iOS 17.3 and iPadOS 17.3. An app may be able to bypass certain Privacy preferences.	2024-01-23	3.3	Low
CVE-2024-21383	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-01-26	3.3	Low
CVE-2023-50785	zohocorp - multiple products	Zoho ManageEngine ADAudit Plus before 7270 allows admin users to view names of arbitrary directories via path traversal.	2024-01-25	2.7	Low
CVE-2024-21336	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-01-26	2.5	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.