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

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 2nd of February to 8th of February. 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**

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

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 ٢ فبراير إلى ٨ فبراير. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدّا: 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
CVE-2025-20124	cisco - multiple products	A vulnerability in an API of Cisco ISE could allow an authenticated, remote attacker to execute arbitrary commands as the root user on an affected device._x000D_ _x000D_ This vulnerability is due to insecure deserialization of user-supplied Java byte streams by the affected software. An attacker could exploit this vulnerability by sending a crafted serialized Java object to an affected API. A successful exploit could allow the attacker to execute arbitrary commands on the device and elevate privileges._x000D_ Note:&nbsp;To successfully exploit this vulnerability, the attacker must have valid read-only administrative credentials. In a single-node deployment, new devices will not be able to authenticate during the reload time.	2025-02-05	9.9
CVE-2024-45569	qualcomm - ar8035_firmware	Memory corruption while parsing the ML IE due to invalid frame content.	2025-02-03	9.8
CVE-2025-0890	zyxel - VMG4325-B10A firmware	**UNSUPPORTED WHEN ASSIGNED** Insecure default credentials for the Telnet function in the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an attacker to log in to the management interface if the administrators have the option to change the default credentials but fail to do so.	2025-02-04	9.8
CVE-2025-1009	mozilla - multiple products	An attacker could have caused a use-after-free via crafted XSLT data, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	9.8
CVE-2025-1016	mozilla - multiple products	Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. 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 < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	9.8
CVE-2025-1017	mozilla - multiple products	Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6. 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 < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	9.8
CVE-2025-1020	mozilla - multiple products	Memory safety bugs present in Firefox 134 and Thunderbird 134. 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 < 135 and Thunderbird < 135.	2025-02-04	9.8
CVE-2025-20125	cisco - multiple products	A vulnerability in an API of Cisco ISE could allow an authenticated, remote attacker with valid read-only credentials to obtain sensitive information, change node configurations, and restart the node._x000D_ _x000D_ This vulnerability is due to a lack of authorization in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted HTTP request to a specific API on the device. A successful exploit could allow the attacker to attacker to obtain information, modify system configuration, and reload the device._x000D_ Note:&nbsp;To successfully exploit this vulnerability, the attacker must have valid read-only administrative credentials. In a single-node deployment, new devices will not be able to authenticate during the reload time.	2025-02-05	9.1

CVE-2024-51450	ibm - Security Verify Directory	IBM Security Verify Directory 10.0.0 through 10.0.3 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request.	2025-02-06	9.1
CVE-2025-23114	veeam - multiple products	A vulnerability in Veeam Updater component allows Man-in-the-Middle attackers to execute arbitrary code on the affected server. This issue occurs due to a failure to properly validate TLS certificate.	2025-02-05	9
CVE-2025-20058	f5 - BIG-IP	When a BIG-IP message routing profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2025-02-05	8.9
CVE-2025-21087	f5 - multiple products	When Client or Server SSL profiles are configured on a Virtual Server, or DNSSEC signing operations are in use, undisclosed traffic can cause an increase in memory and CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2025-02-05	8.9
CVE-2025-24326	f5 - BIG-IP	When BIG-IP Advanced WAF/ASM Behavioral DoS (BADoS) TLS Signatures feature is configured, undisclosed traffic can case an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.9
CVE-2024-38420	qualcomm - aqt1000_firmware	Memory corruption while configuring a Hypervisor based input virtual device.	2025-02-03	8.8
CVE-2024-40890	zyxel - vmg1312-b10a_firmware	**UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.	2025-02-04	8.8
CVE-2024-40891	zyxel - vmg1312-b10a_firmware	**UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.	2025-02-04	8.8
CVE-2025-23015	apache software foundation - Apache Cassandra	Privilege Defined With Unsafe Actions vulnerability in Apache Cassandra. An user with MODIFY permission ON ALL KEYSPACES can escalate privileges to superuser within a targeted Cassandra cluster via unsafe actions to a system resource. Operators granting data MODIFY permission on all keyspaces on affected versions should review data access rules for potential breaches. This issue affects Apache Cassandra through 3.0.30, 3.11.17, 4.0.15, 4.1.7, 5.0.2. Users are recommended to upgrade to versions 3.0.31, 3.11.18, 4.0.16, 4.1.8, 5.0.3, which fixes the issue.	2025-02-04	8.8
CVE-2025-1010	mozilla - multiple products	An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	8.8
CVE-2025-1011	mozilla - multiple products	A bug in WebAssembly code generation could have lead to a crash. It may have been possible for an attacker to leverage this to achieve code execution. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	8.8
CVE-2025-1014	mozilla - multiple products	Certificate length was not properly checked when added to a certificate store. In practice only trusted data was processed. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	8.8
CVE-2025-23058	hewlett packard enterprise (hpe) - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the ClearPass Policy Manager web-based management interface allows a low-privileged (read-only) authenticated remote attacker to gain unauthorized access to data and the ability to execute functions that should be restricted to administrators only with read/write privileges. Successful exploitation could enable a low-privileged user to execute administrative functions leading to an escalation of privileges.	2025-02-04	8.8
CVE-2025-21342	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2025-02-06	8.8
CVE-2025-21408	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2025-02-06	8.8
CVE-2025-20029	f5 - BIG-IP	Command injection vulnerability exists in iControl REST and BIG-IP TMOS Shell (tmsh) save command, which may allow an authenticated attacker to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-20045	f5 - BIG-IP	When SIP session Application Level Gateway mode (ALG) profile with Passthru Mode enabled and SIP router ALG profile are configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-21091	f5 - BIG-IP	When SNMP v1 or v2c are disabled on the BIG-IP, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2025-02-05	8.7

CVE-2025-22846	f5 - multiple products	When SIP Session and Router ALG profiles are configured on a Message Routing type virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-22891	f5 - BIG-IP	When BIG-IP PEM Control Plane listener Virtual Server is configured with Diameter Endpoint profile, undisclosed traffic can cause the Virtual Server to stop processing new client connections and an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-23412	f5 - BIG-IP	When BIG-IP APM Access Profile is configured on a virtual server, undisclosed request can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-24312	f5 - multiple products	When BIG-IP AFM is provisioned with IPS module enabled and protocol inspection profile is configured on a virtual server or firewall rule or policy, undisclosed traffic can cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-24497	f5 - BIG-IP	When URL categorization is configured on a virtual server, undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.7
CVE-2025-21177	microsoft - dynamics_365_sales	Server-Side Request Forgery (SSRF) in Microsoft Dynamics 365 Sales allows an authorized attacker to elevate privileges over a network.	2025-02-06	8.7
CVE-2024-37358	apache software foundation - Apache James server	Similarly to CVE-2024-34055, Apache James is vulnerable to denial of service through the abuse of IMAP literals from both authenticated and unauthenticated users, which could be used to cause unbounded memory allocation and very long computations Version 3.7.6 and 3.8.2 restrict such illegitimate use of IMAP literals.	2025-02-06	8.6
CVE-2025-23239	f5 - BIG-IP	When running in Appliance mode, an authenticated remote command injection vulnerability exists in an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	8.5
CVE-2022-31764	apache software foundation - Apache ShardingSphere ElasticJob-UI	The Lite UI of Apache ShardingSphere ElasticJob-UI allows an attacker to perform RCE by constructing a special JDBC URL of H2 database. This issue affects Apache ShardingSphere ElasticJob-UI version 3.0.1 and prior versions. This vulnerability has been fixed in ElasticJob-UI 3.0.2. The premise of this attack is that the attacker has obtained the account and password. Otherwise, the attacker cannot perform this attack.	2025-02-06	8.5
CVE-2024-49838	qualcomm - ar8035_firmware	Information disclosure while parsing the OCI IE with invalid length.	2025-02-03	8.2
CVE-2024-49839	qualcomm - ar8035_firmware	Memory corruption during management frame processing due to mismatch in T2LM info element.	2025-02-03	8.2
CVE-2025-25246	netgear - multiple products	NETGEAR XR1000 before 1.0.0.74, XR1000v2 before 1.1.0.22, and XR500 before 2.3.2.134 allow remote code execution by unauthenticated users.	2025-02-05	8.1
CVE-2024-38418	qualcomm - c-v2x_9150_firmware	Memory corruption while parsing the memory map info in IOCTL calls.	2025-02-03	7.8
CVE-2024-45560	qualcomm - aqt1000_firmware	Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.	2025-02-03	7.8
CVE-2024-45561	qualcomm - aqt1000_firmware	Memory corruption while handling IOCTL call from user-space to set latency level.	2025-02-03	7.8
CVE-2024-45571	qualcomm - ar8035_firmware	Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.	2025-02-03	7.8
CVE-2024-45573	qualcomm - fastconnect_6700_firmware	Memory corruption may occour while generating test pattern due to negative indexing of display ID.	2025-02-03	7.8
CVE-2024-45582	qualcomm - fastconnect_6900_firmware	Memory corruption while validating number of devices in Camera kernel .	2025-02-03	7.8
CVE-2024-45584	qualcomm - ar8035_firmware	Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.	2025-02-03	7.8
CVE-2024-49832	qualcomm - fastconnect_6900_firmware	Memory corruption in Camera due to unusually high number of nodes passed to AXI port.	2025-02-03	7.8
CVE-2024-49833	qualcomm - fastconnect_6700_firmware	Memory corruption can occur in the camera when an invalid CID is used.	2025-02-03	7.8

CVE-2024-49834	qualcomm - csra6620_firmware	Memory corruption while power-up or power-down sequence of the camera sensor.	2025-02-03	7.8
CVE-2024-49837	qualcomm - qam8255p_firmware	Memory corruption while reading CPU state data during guest VM suspend.	2025-02-03	7.8
CVE-2024-49840	qualcomm - fastconnect_6900_firmware	Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.	2025-02-03	7.8
CVE-2024-49843	qualcomm - fastconnect_6200_firmware	Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.	2025-02-03	7.8
CVE-2024-49814	ibm - Security Verify Access Appliance	IBM Security Verify Access Appliance 10.0.0 through 10.0.3 could allow a locally authenticated user to increase their privileges due to execution with unnecessary privileges.	2025-02-06	7.8
CVE-2025-20169	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2025-20170	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2025-20171	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2025-20172	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software, Cisco IOS XE Software, and Cisco IOS XR Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. For Cisco IOS and IOS XE Software, a successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. For Cisco IOS XR Software, a successful exploit could allow the attacker to cause the SNMP process to restart, resulting in an interrupted SNMP response from an affected device. Devices that are running Cisco IOS XR Software will not reload.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2025-20173	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2025-20174	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS	2025-02-05	7.7

		condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.		
CVE-2025-20175	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2025-20176	cisco - multiple products	A vulnerability in the SNMP subsystem of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a DoS condition on an affected device._x000D_ _x000D_ This vulnerability is due to improper error handling when parsing SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.&nbsp;_x000D_ This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMP v2c or earlier, the attacker must know a valid read-write or read-only SNMP community string for the affected system. To exploit this vulnerability through SNMP v3, the attacker must have valid SNMP user credentials for the affected system.	2025-02-05	7.7
CVE-2024-57960	huawei - multiple products	Input verification vulnerability in the ExternalStorageProvider module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-02-06	7.7
CVE-2024-38404	qualcomm - ar8035_firmware	Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.	2025-02-03	7.5
CVE-2025-1012	mozilla - multiple products	A race during concurrent delazification could have led to a use-after-free. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	7.5
CVE-2024-23690	netgear - multiple products	The end-of-life Netgear FVS336Gv2 and FVS336Gv3 are affected by a command injection vulnerability in the Telnet interface. An authenticated and remote attacker can execute arbitrary OS commands as root over Telnet by sending crafted "util backup_configuration" commands.	2025-02-04	7.2
CVE-2024-49352	ibm - Cognos Analytics	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, 12.0.2, 12.0.3, and 12.0.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2025-02-05	7.1
CVE-2025-24319	f5 - BIG-IP Next Central Manager	When BIG-IP Next Central Manager is running, undisclosed requests to the BIG-IP Next Central Manager API can cause the BIG-IP Next Central Manager Node's Kubernetes service to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	7.1
CVE-2024-54171	ibm - EntireX	IBM EntireX 11.1 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. An authenticated attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2025-02-06	7.1
CVE-2025-1103	d-link - DIR-823X	A vulnerability, which was classified as problematic, was found in D-Link DIR-823X 240126/240802. This affects the function set_wifi_blacklists of the file /goform/set_wifi_blacklists of the component HTTP POST Request Handler. The manipulation of the argument macList leads to null pointer dereference. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-02-07	7.1
CVE-2025-20881	samsung - multiple products	Out-of-bounds write in accessing buffer storing the decoded video frames in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.	2025-02-04	7
CVE-2025-20882	samsung - multiple products	Out-of-bounds write in accessing uninitialized memory for svc1td in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.	2025-02-04	7
CVE-2025-20888	samsung - multiple products	Out-of-bounds write in handling the block size for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.	2025-02-04	7
CVE-2025-20890	samsung - multiple products	Out-of-bounds write in decoding frame buffer in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.	2025-02-04	7
CVE-2025-1104	d-link - DHP-W310AV	A vulnerability has been found in D-Link DHP-W310AV 1.04 and classified as critical. This vulnerability affects unknown code. The manipulation leads to authentication bypass by spoofing. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-02-07	6.9
CVE-2025-23059	hewlett packard enterprise (hpe) - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the web-based management interface of HPE Aruba Networking ClearPass Policy Manager exposes directories containing sensitive information. If exploited successfully, this vulnerability allows an authenticated remote attacker with high privileges to access and retrieve sensitive data, potentially compromising the integrity and security of the entire system.	2025-02-04	6.8

CVE-2024-57961	huawei - multiple products	Out-of-bounds write vulnerability in the emcom module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-02-06	6.8
CVE-2025-20636	google - multiple products	In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.	2025-02-03	6.7
CVE-2025-23413	f5 - BIG-IP Next Central Manager	When users log in through the webUI or API using local authentication, BIG-IP Next Central Manager may log sensitive information in the pgaudit log files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	6.7
CVE-2024-20141	google - multiple products	In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.	2025-02-03	6.6
CVE-2024-20142	google - multiple products	In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.	2025-02-03	6.6
CVE-2025-20639	google - multiple products	In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.	2025-02-03	6.6
CVE-2025-20641	google - multiple products	In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.	2025-02-03	6.6
CVE-2025-20642	google - multiple products	In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.	2025-02-03	6.6
CVE-2024-38411	qualcomm - fastconnect_6900_firmware	Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.	2025-02-03	6.6
CVE-2024-38412	qualcomm - fastconnect_7800_firmware	Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.	2025-02-03	6.6
CVE-2024-38413	qualcomm - fastconnect_7800_firmware	Memory corruption while processing frame packets.	2025-02-03	6.6
CVE-2025-23060	hewlett packard enterprise (hpe) - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in HPE Aruba Networking ClearPass Policy Manager may, under certain circumstances, expose sensitive unencrypted information. Exploiting this vulnerability could allow an attacker to perform a man-in-the-middle attack, potentially granting unauthorized access to network resources as well as enabling data tampering.	2025-02-04	6.6
CVE-2025-21117	dell - Avamar	Dell Avamar, version 19.4 or later, contains an access token reuse vulnerability in the AUI. A low privileged local attacker could potentially exploit this vulnerability, leading to fully impersonating the user.	2025-02-05	6.6
CVE-2024-57957	huawei - HarmonyOS	Vulnerability of improper log information control in the UI framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-02-06	6.6
CVE-2025-0510	mozilla - multiple products	Thunderbird displayed an incorrect sender address if the From field of an email used the invalid group name syntax that is described in CVE-2024-49040. This vulnerability affects Thunderbird < 128.7 and Thunderbird < 135.	2025-02-04	6.5
CVE-2025-1013	mozilla - multiple products	A race condition could have led to private browsing tabs being opened in normal browsing windows. This could have resulted in a potential privacy leak. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.	2025-02-04	6.5
CVE-2024-35138	ibm - multiple products	IBM Security Verify Access Appliance and Container 10.0.0 through 10.0.8 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2025-02-04	6.5
CVE-2025-20184	cisco - multiple products	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email Gateway and Cisco Secure Web Appliance could allow an authenticated, remote attacker to perform command injection attacks against an affected device. The attacker must authenticate with valid administrator credentials._x000D_ _x000D_ This vulnerability is due to insufficient validation of XML configuration files by an affected device. An attacker could exploit this vulnerability by uploading a crafted XML configuration file. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	2025-02-05	6.5
CVE-2025-0799	ibm - IBM App Connect Enterprise	IBM App Connect enterprise 12.0.1.0 through 12.0.12.10 and 13.0.1.0 through 13.0.2.1 could allow an authenticated user to write to an arbitrary file on the system during bar configuration deployment due to improper pathname limitations on restricted directories.	2025-02-06	6.5
CVE-2024-45626	apache - multiple products	Apache James server JMAP HTML to text plain implementation in versions below 3.8.2 and 3.7.6 is subject to unbounded memory consumption that can result in a denial of service. Users are recommended to upgrade to version 3.7.6 and 3.8.2, which fix this issue.	2025-02-06	6.5
CVE-2025-21279	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2025-02-06	6.5
CVE-2025-21283	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2025-02-06	6.5

CVE-2025-25069	apache software foundation - Apache Kvrocks	A Cross-Protocol Scripting vulnerability is found in Apache Kvrocks. Since Kvrocks didn't detect if "Host:" or "POST" appears in RESP requests, a valid HTTP request can also be sent to Kvrocks as a valid RESP request and trigger some database operations, which can be dangerous when it is chained with SSRF. It is similiar to CVE-2016-10517 in Redis. This issue affects Apache Kvrocks: from the initial version to the latest version 2.11.0. Users are recommended to upgrade to version 2.11.1, which fixes the issue.	2025-02-07	6.5
CVE-2025-20885	samsung - multiple products	Out-of-bounds write in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to cause memory corruption.	2025-02-04	6.4
CVE-2024-52365	ibm - Cloud Pak for Business Automation	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-05	6.4
CVE-2024-56472	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-05	6.4
CVE-2024-49791	ibm - applinx	IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-06	6.4
CVE-2025-20904	samsung - multiple products	Out-of-bounds write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to cause memory corruption.	2025-02-04	6.3
CVE-2025-20905	samsung - multiple products	Out-of-bounds read and write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to read and write out-of-bounds memory.	2025-02-04	6.3
CVE-2025-0444	google - Chrome	Use after free in Skia in Google Chrome prior to 133.0.6943.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-02-04	6.3
CVE-2025-0451	google - Chrome	Inappropriate implementation in Extensions API in Google Chrome prior to 133.0.6943.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Medium)	2025-02-04	6.3
CVE-2023-52925	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: don't fail inserts if duplicate has expired nftables selftests fail: run-tests.sh testcases/sets/0044interval_overlap_0 Expected: 0-2 . 0-3, got: W: [FAILED] ./testcases/sets/0044interval_overlap_0: got 1 Insertion must ignore duplicate but expired entries. Moreover, there is a strange asymmetry in nft_pipapo_activate: It refetches the current element, whereas the other ->activate callbacks (bitmap, hash, rhash, rbtree) use elem->priv. Same for .remove: other set implementations take elem->priv, nft_pipapo_remove fetches elem->priv, then does a relookup, remove this. I suspect this was the reason for the change that prompted the removal of the expired check in pipapo_get() in the first place, but skipping exired elements there makes no sense to me, this helper is used for normal get requests, insertions (duplicate check) and deactivate callback. In first two cases expired elements must be skipped. For ->deactivate(), this gets called for DELSETELEM, so it seems to me that expired elements should be skipped as well, i.e. delete request should fail with -ENOENT error.	2025-02-05	6.2
CVE-2024-12602	huawei - HarmonyOS	Identity verification vulnerability in the ParamWatcher module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-02-06	6.2
CVE-2024-57954	huawei - HarmonyOS	Permission verification vulnerability in the media library module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-02-06	6.2
CVE-2024-38414	qualcomm - fastconnect_6900_firmware	Information disclosure while processing information on firmware image during core initialization.	2025-02-03	6.1
CVE-2024-38416	qualcomm - ar8035_firmware	Information disclosure during audio playback.	2025-02-03	6.1
CVE-2024-38417	qualcomm - ar8035_firmware	Information disclosure while processing IO control commands.	2025-02-03	6.1
CVE-2024-40700	ibm - multiple products	IBM Security Verify Access Appliance and Container 10.0.0 through 10.0.8 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in	2025-02-04	6.1

		the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.		
CVE-2025-20179	cisco - Cisco TelePresence Video Communication Server (VCS) Expressway	A vulnerability in the web-based management interface of Cisco Expressway Series could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface._x000D_ _x000D_ 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._x000D_ Note:&nbsp;Cisco Expressway Series refers to Cisco Expressway Control (Expressway-C) devices and Cisco Expressway Edge (Expressway-E) devices.	2025-02-05	6.1
CVE-2024-57955	huawei - HarmonyOS	Arbitrary write vulnerability in the Gallery module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-02-06	6.1
CVE-2024-57959	huawei - multiple products	Use-After-Free (UAF) vulnerability in the display module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-02-06	6.1
CVE-2024-57962	huawei - HarmonyOS	Vulnerability of incomplete verification information in the VPN service module Impact: Successful exploitation of this vulnerability may affect availability.	2025-02-06	6.1
CVE-2024-52892	ibm - Jazz for Service Management	IBM Jazz for Service Management 1.1.3 through 1.1.3.23 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-06	6.1
CVE-2025-20907	samsung - multiple products	Improper privilege management in Samsung Find prior to SMR Feb-2025 Release 1 allows local privileged attackers to disable Samsung Find.	2025-02-04	6
CVE-2025-20892	samsung - multiple products	Protection Mechanism Failure in bootloader prior to SMR Jan-2025 Release 1 allows physical attackers to allow to execute fastboot command. User interaction is required for triggering this vulnerability.	2025-02-04	5.9
CVE-2024-43187	ibm - multiple products	IBM Security Verify Access Appliance and Container 10.0.0 through 10.0.8 transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.	2025-02-04	5.9
CVE-2024-49797	ibm - applinx	IBM ApplinX 11.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	2025-02-06	5.9
CVE-2025-20183	cisco - Cisco Secure Web Appliance	A vulnerability in a policy-based Cisco Application Visibility and Control (AVC) implementation of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to evade the antivirus scanner and download a malicious file onto an endpoint.&nbsp;_x000D_ _x000D_ The vulnerability is due to improper handling of a crafted range request header. An attacker could exploit this vulnerability by sending an HTTP request with a crafted range request header through the affected device. A successful exploit could allow the attacker to evade the antivirus scanner and download malware onto the endpoint without detection by Cisco Secure Web Appliance.	2025-02-05	5.8
CVE-2024-57958	huawei - multiple products	Out-of-bounds array read vulnerability in the FFRT module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-02-06	5.7
CVE-2025-0158	ibm - EntireX	IBM EntireX 11.1 could allow a local user to cause a denial of service due to an unhandled error and fault isolation.	2025-02-06	5.5
CVE-2025-24860	apache software foundation - Apache Cassandra	Incorrect Authorization vulnerability in Apache Cassandra allowing users to access a datacenter or IP/CIDR groups they should not be able to when using CassandraNetworkAuthorizer or CassandraCIDRAuthorizer. Users with restricted data center access can update their own permissions via data control language (DCL) statements on affected versions. This issue affects Apache Cassandra: from 4.0.0 through 4.0.15 and from 4.1.0 through 4.1.7 for CassandraNetworkAuthorizer, and from 5.0.0 through 5.0.2 for both CassandraNetworkAuthorizer and CassandraCIDRAuthorizer. Operators using CassandraNetworkAuthorizer or CassandraCIDRAuthorizer on affected versions should review data access rules for potential breaches. Users are recommended to upgrade to versions 4.0.16, 4.1.8, 5.0.3, which fixes the issue.	2025-02-04	5.4
CVE-2025-1015	mozilla - thunderbird	The Thunderbird Address Book URI fields contained unsanitized links. This could be used by an attacker to create and export an address book containing a malicious payload in a field. For example, in the "Other" field of the Instant Messaging section. If another user imported the address book, clicking on the link could result in opening a web page inside Thunderbird, and that page could execute (unprivileged) JavaScript. This vulnerability affects Thunderbird < 128.7.	2025-02-04	5.4
CVE-2024-48019	apache software foundation - Apache Doris	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Files or Directories Accessible to External Parties vulnerability in Apache Doris. Application administrators can read arbitrary files from the server filesystem through path traversal. Users are recommended to upgrade to version 2.1.8, 3.0.3 or later, which fixes the issue.	2025-02-04	5.4

CVE-2025-0445	google - Chrome	Use after free in V8 in Google Chrome prior to 133.0.6943.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2025-02-04	5.4
CVE-2024-53962	adobe - multiple products	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2025-02-05	5.4
CVE-2024-53963	adobe - multiple products	Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privileged attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. This type of attack requires user interaction, as the victim would need to access a manipulated link or input data into a vulnerable page.	2025-02-05	5.4
CVE-2024-53964	adobe - multiple products	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2025-02-05	5.4
CVE-2024-53965	adobe - multiple products	Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a low privileged attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. This type of attack requires user interaction, as the victim would need to access a manipulated link or input data into a vulnerable page.	2025-02-05	5.4
CVE-2024-53966	adobe - multiple products	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2025-02-05	5.4
CVE-2024-52364	ibm - Cloud Pak for Business Automation	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-05	5.4
CVE-2024-56470	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2025-02-05	5.4
CVE-2024-56471	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2025-02-05	5.4
CVE-2024-49792	ibm - applinx	IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-06	5.4
CVE-2024-49793	ibm - applinx	IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-06	5.4
CVE-2024-49796	ibm - applinx	IBM ApplinX 11.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim.	2025-02-06	5.4
CVE-2025-20887	samsung - multiple products	Out-of-bounds read in accessing table used for svp8t in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.	2025-02-04	5.3
CVE-2025-20889	samsung - multiple products	Out-of-bounds read in decoding malformed bitstream for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.	2025-02-04	5.3
CVE-2025-20891	samsung - multiple products	Out-of-bounds read in decoding malformed bitstream of video thumbnails in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.	2025-02-04	5.3
CVE-2024-27137	apache software foundation - Apache Cassandra	In Apache Cassandra it is possible for a local attacker without access to the Apache Cassandra process or configuration files to manipulate the RMI registry to perform a man-in-the-middle attack and capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and perform unauthorized operations. This is same vulnerability that CVE-2020-13946 was issued for, but the Java option was changed in JDK10. This issue affects Apache Cassandra from 4.0.2 through 5.0.2 running Java 11. Operators are recommended to upgrade to a release equal to or later than 4.0.15, 4.1.8, or 5.0.3 which fixes the issue.	2025-02-04	5.3
CVE-2025-1018	mozilla - multiple products	The fullscreen notification is prematurely hidden when fullscreen is re-requested quickly by the user. This could have been leveraged to perform a potential spoofing attack. This vulnerability affects Firefox < 135 and Thunderbird < 135.	2025-02-04	5.3
CVE-2024-45659	ibm - multiple products	IBM Security Verify Access Appliance and Container 10.0.0 through 10.0.8 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-04	5.3
CVE-2025-23419	f5 - multiple products	When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This	2025-02-05	5.3

		vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
CVE-2024-56473	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 could allow an attacker to spoof their IP address, which is written to log files, due to improper verification of 'Client-IP' headers.	2025-02-05	5.3
CVE-2025-21253	microsoft - multiple products	Microsoft Edge for IOS and Android Spoofing Vulnerability	2025-02-06	5.3
CVE-2025-20893	samsung - multiple products	Improper access control in NotificationManager prior to SMR Jan-2025 Release 1 allows local attackers to change the configuration of notifications.	2025-02-04	5.1
CVE-2025-24320	f5 - BIG-IP	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. This vulnerability is due to an incomplete fix for CVE-2024-31156 https://my.f5.com/manage/s/article/K000138636 . Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	5.1
CVE-2024-45657	ibm - multiple products	IBM Security Verify Access Appliance and Container 10.0.0 through 10.0.8 could allow a local privileged user to perform unauthorized actions due to incorrect permissions assignment.	2025-02-04	5
CVE-2025-20180	cisco - multiple products	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager and Secure Email Gateway could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface._x000D_ _x000D_ This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected 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. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Operator.	2025-02-05	4.8
CVE-2025-20204	cisco - Cisco Identity Services Engine Software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface.&nbsp;_x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. 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. To exploit this vulnerability, the attacker must have valid administrative credentials.	2025-02-05	4.8
CVE-2025-20205	cisco - Cisco Identity Services Engine Software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface.&nbsp;_x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. 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. To exploit this vulnerability, the attacker must have valid administrative credentials.	2025-02-05	4.8
CVE-2024-38317	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-05	4.8
CVE-2024-38318	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	2025-02-05	4.8
CVE-2025-25039	hewlett packard enterprise (hpe) - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the web-based management interface of HPE Aruba Networking ClearPass Policy Manager (CPPM) allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system.	2025-02-04	4.7
CVE-2025-20883	samsung - multiple products	Improper access control in SoundPicker prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.	2025-02-04	4.6
CVE-2025-20884	samsung - multiple products	Improper access control in Samsung Message prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.	2025-02-04	4.6
CVE-2025-21267	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2025-02-06	4.4
CVE-2025-20638	google - multiple products	In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.	2025-02-03	4.3
CVE-2025-20640	google - multiple products	In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.	2025-02-03	4.3
CVE-2025-1019	mozilla - multiple products	The z-order of the browser windows could be manipulated to hide the fullscreen notification. This could potentially be leveraged to perform a spoofing attack. This vulnerability affects Firefox < 135 and Thunderbird < 135.	2025-02-04	4.3

CVE-2024-49348	ibm - Cloud Pak for Business Automation	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 allows restricting access to organizational data to valid contexts. The fact that tasks of type comment can be reassigned via API implicitly grants access to user queries in an unexpected context.	2025-02-05	4.3
CVE-2025-20207	cisco - multiple products	A vulnerability in Simple Network Management Protocol (SNMP) polling for Cisco Secure Email and Web Manager, Cisco Secure Email Gateway, and Cisco Secure Web Appliance could allow an authenticated, remote attacker to obtain confidential information about the underlying operating system._x000D_ _x000D_ This vulnerability exists because the appliances do not protect confidential information at rest in response to SNMP poll requests. An attacker could exploit this vulnerability by sending a crafted SNMP poll request to the affected appliance. A successful exploit could allow the attacker to discover confidential information that should be restricted. To exploit this vulnerability, an attacker must have the configured SNMP credentials.	2025-02-05	4.3
CVE-2024-38316	ibm - Aspera Shares	IBM Aspera Shares 1.9.0 through 1.10.0 PL6 does not properly rate limit the frequency that an authenticated user can send emails, which could result in email flooding or a denial of service.	2025-02-05	4.3
CVE-2024-49794	ibm - applinx	IBM ApplinX 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2025-02-06	4.3
CVE-2024-49795	ibm - applinx	IBM ApplinX 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2025-02-06	4.3
CVE-2024-49798	ibm - applinx	IBM ApplinX 11.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2025-02-06	4.3
CVE-2024-49800	ibm - applinx	IBM ApplinX 11.1 stores sensitive information in cleartext in memory that could be obtained by an authenticated user.	2025-02-06	4.3
CVE-2025-21404	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2025-02-06	4.3
CVE-2024-54176	ibm - multiple products	IBM DevOps Deploy 8.0 through 8.0.1.4, 8.1 through 8.1.0.0 and IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.25, 7.1 through 7.1.2.21, 7.2 through 7.2.3.14 and 7.3 through 7.3.2 could allow an authenticated user to obtain sensitive information about other users on the system due to missing authorization for a function.	2025-02-08	4.3
CVE-2025-20886	samsung - multiple products	Inclusion of sensitive information in test code in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to get test key.	2025-02-04	4.1
CVE-2025-20643	google - multiple products	In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.	2025-02-03	3.9
CVE-2025-22475	dell - multiple products	Dell PowerProtect DD, versions prior to DDOS 8.3.0.0, 7.10.1.50, and 7.13.1.10 contains a use of a Cryptographic Primitive with a Risky Implementation vulnerability. A remote attacker could potentially exploit this vulnerability, leading to Information tampering.	2025-02-04	3.7
CVE-2024-9097	manageengine - Endpoint Central	ManageEngine Endpoint Central versions before 11.3.2440.09 are vulnerable to IDOR vulnerability which allows the attacker to change the username in the chat.	2025-02-05	3.5
CVE-2025-20185	cisco - multiple products	A vulnerability in the implementation of the remote access functionality of Cisco AsyncOS Software for Cisco Secure Email and Web Manager, Cisco Secure Email Gateway, and Cisco Secure Web Appliance could allow an authenticated, local attacker to elevate privileges to root. The attacker must authenticate with valid administrator credentials._x000D_ _x000D_ This vulnerability is due to an architectural flaw in the password generation algorithm for the remote access functionality. An attacker could exploit this vulnerability by generating a temporary password for the service account. A successful exploit could allow the attacker to execute arbitrary commands as root and access the underlying operating system._x000D_ Note: The Security Impact Rating (SIR) for this vulnerability is Medium due to the unrestricted scope of information that is accessible to an attacker.	2025-02-05	3.4
CVE-2024-56467	ibm - EntireX	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-06	3.3
CVE-2024-57956	huawei - HarmonyOS	Out-of-bounds read vulnerability in the interpreter string module Impact: Successful exploitation of this vulnerability may affect availability.	2025-02-06	2.8
CVE-2024-45658	ibm - multiple products	IBM Security Verify Access Appliance and Container 10.0.0 through 10.0.8 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-04	2.7
CVE-2025-22402	dell - Update Manager Plugin	Dell Update Manager Plugin, version(s) 1.5.0 through 1.6.0, contain(s) an Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2025-02-07	2.6
CVE-2025-23415	f5 - BIG-IP	An insufficient verification of data authenticity vulnerability exists in BIG-IP APM Access Policy endpoint inspection that may allow an attacker to bypass endpoint inspection checks for VPN connection initiated thru BIG-IP APM browser network access VPN client for Windows, macOS and Linux. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-02-05	2.3
CVE-2025-24959	google - zx	zx is a tool for writing better scripts. An attacker with control over environment variable values can inject unintended environment variables into `process.env`. This can lead to arbitrary command	2025-02-03	1

		execution or unexpected behavior in applications that rely on environment variables for security-sensitive operations. Applications that process untrusted input and pass it through `dotenv.stringify` are particularly vulnerable. This issue has been patched in version 8.3.2. Users should immediately upgrade to this version to mitigate the vulnerability. If upgrading is not feasible, users can mitigate the vulnerability by sanitizing user-controlled environment variable values before passing them to `dotenv.stringify`. Specifically, avoid using `"`, `'`, and backticks in values, or enforce strict validation of environment variables before usage.		

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.