الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority

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

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 ٤th of May to 10th of May. 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 4 مايو إلى ١٠ مايو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

| CVE ID & Source | Vendor - Product | Description | Publish Date | CVSS Score |
|---|---|---|---|---|
| CVE-2025-20188 | cisco - Cisco IOS XE Software | A vulnerability in the Out-of-Band Access Point (AP) Image Download feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system. This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system. An attacker could exploit this vulnerability by sending crafted HTTPS requests to the AP image download interface. A successful exploit could allow the attacker to upload files, perform path traversal, and execute arbitrary commands with root privileges. Note: For exploitation to be successful, the Out-of-Band AP Image Download feature must be enabled on the device. It is not enabled by default. | 2025-05-07 | 10.0 |
| CVE-2025-29813 | microsoft - Azure DevOps | [Spoofable identity claims] Authentication Bypass by Assumed-Immutable Data in Azure DevOps allows an unauthorized attacker to elevate privileges over a network. | 2025-05-08 | 10.0 |
| CVE-2025-29827 | microsoft - Azure Automation | Improper Authorization in Azure Automation allows an authorized attacker to elevate privileges over a network. | 2025-05-08 | 9.9 |
| CVE-2025-29972 | microsoft - Azure Storage Resource Provider (SRP) | Server-Side Request Forgery (SSRF) in Azure allows an authorized attacker to perform spoofing over a network. | 2025-05-08 | 9.9 |
| CVE-2024-57229 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the devname parameter in the reset_wifi function. | 2025-05-05 | 9.8 |
| CVE-2024-57230 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_do_enr_pin_wps function. | 2025-05-05 | 9.8 |
| CVE-2024-57231 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_do_enr_pbc_wps function. | 2025-05-05 | 9.8 |
| CVE-2024-57232 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_wps_gen_pincode function. | 2025-05-05 | 9.8 |
| CVE-2024-57233 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) v1.0.2.26 was discovered to contain a command injection vulnerability via the iface parameter in the vif_disable function. | 2025-05-05 | 9.8 |
| CVE-2024-57234 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the ifname parameter in the apcli_cancel_wps function. | 2025-05-05 | 9.8 |
| CVE-2024-57235 | netgear - rax50_firmware | NETGEAR RAX5 (AX1600 WiFi Router) V1.0.2.26 was discovered to contain a command injection vulnerability via the iface parameter in the vif_enable function. | 2025-05-05 | 9.8 |
| CVE-2025-4052 | google - Chrome | Inappropriate implementation in DevTools in Google Chrome prior to 136.0.7103.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low) | 2025-05-05 | 9.8 |
| CVE-2025-45492 | netgear - ex8000_firmware | Netgear EX8000 V1.0.0.126 is vulnerable to Command Injection via the Iface parameter in the action_wireless function. | 2025-05-06 | 9.8 |
| CVE-2025-36546 | f5 - multiple products | On an F5OS system, if the root user had previously configured the system to allow login via SSH key-based authentication, and then enabled Appliance Mode; access via SSH key-based authentication is still allowed. For an attacker to exploit this vulnerability they must obtain the root user's SSH private key.  Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 9.2 |
| CVE-2025-2905 | wso2 - WSO2 API Manager | An XML External Entity (XXE) vulnerability exists in the gateway component of WSO2 API Manager due to insufficient validation of XML input in crafted URL paths. User-supplied XML is parsed without appropriate restrictions, enabling external entity resolution.This vulnerability can be exploited by an unauthenticated remote attacker to read files from the server’s filesystem or perform denial-of-service (DoS) attacks.<br>On systems running JDK 7 or early JDK 8, full file contents may be exposed.<br>On later versions of JDK 8 and newer, only the first line of a file may be read, due to improvements | 2025-05-05 | 9.1 |

| | | | | |
|---|---|---|---|---|
| | | in XML parser behavior.<br>DoS attacks such as "Billion Laughs" payloads can cause service disruption. | | |
| CVE-2025-47733 | microsoft - Microsoft Power Apps | Server-Side Request Forgery (SSRF) in Microsoft Power Apps allows an unauthorized attacker to disclose information over a network | 2025-05-08 | 9.1 |
| CVE-2025-0649 | google - Tensorflow | Incorrect JSON input stringification in Google's Tensorflow serving versions up to 2.18.0 allows for potentially unbounded recursion leading to server crash. | 2025-05-06 | 8.9 |
| CVE-2025-4050 | google - Chrome | Out of bounds memory access in DevTools in Google Chrome prior to 136.0.7103.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) | 2025-05-05 | 8.8 |
| CVE-2025-4096 | google - Chrome | Heap buffer overflow in HTML in Google Chrome prior to 136.0.7103.59 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) | 2025-05-05 | 8.8 |
| CVE-2025-4372 | google - Chrome | Use after free in WebAudio in Google Chrome prior to 136.0.7103.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) | 2025-05-06 | 8.8 |
| CVE-2025-20186 | cisco - Cisco IOS XE Software | A vulnerability in the web-based management interface of the Wireless LAN Controller feature of Cisco IOS XE Software could allow an authenticated, remote attacker with a lobby ambassador user account to perform a command injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary Cisco IOS XE Software CLI commands with privilege level 15. Note: This vulnerability is exploitable only if the attacker obtains the credentials for a lobby ambassador account. This account is not configured by default. | 2025-05-07 | 8.8 |
| CVE-2025-32819 | sonicwall - SMA100 | A vulnerability in SMA100 allows a remote authenticated attacker with SSLVPN user privileges to bypass the path traversal checks and delete an arbitrary file potentially resulting in a reboot to factory default settings. | 2025-05-07 | 8.8 |
| CVE-2025-35995 | f5 - BIG-IP | When a BIG-IP PEM system is licensed with URL categorization, and the URL categorization policy or an iRule with the urlcat command is enabled on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-36504 | f5 - multiple products | When a BIG-IP HTTP/2 httprouter profile is configured on a virtual server, undisclosed responses can cause an increase in memory resource utilization.  Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-36525 | f5 - BIG-IP | When a BIG-IP APM virtual server is configured to use a PingAccess profile, undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-36557 | f5 - multiple products | When an HTTP profile with the Enforce RFC Compliance option is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-41399 | f5 - multiple products | When a Stream Control Transmission Protocol (SCTP) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-41414 | f5 - multiple products | When HTTP/2 client and server profile 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 | 2025-05-07 | 8.7 |
| CVE-2025-41431 | f5 - BIG-IP | When connection mirroring is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate in the standby BIG-IP systems in a traffic group. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-41433 | f5 - BIG-IP | When a Session Initiation Protocol (SIP) message routing framework (MRF) application layer gateway (ALG) profile is configured on a Message Routing virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-46265 | f5 - multiple products | On F5OS, an improper authorization vulnerability exists where remotely authenticated users (LDAP, RADIUS, TACACS+) may be authorized with higher privilege F5OS roles. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.7 |
| CVE-2025-47732 | microsoft - Microsoft Dataverse | Microsoft Dataverse Remote Code Execution Vulnerability | 2025-05-08 | 8.7 |
| CVE-2025-20154 | cisco - Cisco IOS XR Software | A vulnerability in the Two-Way Active Measurement Protocol (TWAMP) server feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. For Cisco IOS XR Software, this vulnerability could cause the ipsla_ippm_server&nbsp;process to reload unexpectedly if debugs are enabled. This vulnerability is due to out-of-bounds array access when processing specially crafted TWAMP control packets. An attacker could exploit this vulnerability by sending crafted TWAMP control packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: For Cisco IOS XR Software, only the ipsla_ippm_server process reloads unexpectedly and only when debugs are enabled. The vulnerability details for Cisco IOS XR Software are as follows:&nbsp;&nbsp;&nbsp;&nbsp;Security Impact Rating (SIR): Low&nbsp;&nbsp;&nbsp;&nbsp;CVSS Base Score: 3.7&nbsp;&nbsp;&nbsp;&nbsp;CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L | 2025-05-07 | 8.6 |
| CVE-2025-20162 | cisco - Cisco IOS XE Software | A vulnerability in the DHCP snooping security feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a full interface queue wedge, which could result in a denial of service (DoS) condition. This vulnerability is due to improper handling of DHCP request packets. An attacker could exploit this vulnerability by sending DHCP request packets to an affected device. A successful exploit could allow the attacker to cause packets to wedge in the queue, creating a DoS condition for downstream devices of the affected system and requiring that the system restart to drain the queue. Note: This vulnerability can be exploited with either unicast or broadcast DHCP packets on a VLAN that does not have DHCP snooping enabled. | 2025-05-07 | 8.6 |

| | | | | |
|---|---|---|---|---|
| CVE-2025-20182 | cisco - multiple products | A vulnerability in the Internet Key Exchange version 2 (IKEv2) protocol processing of Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco IOS Software, and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation when processing IKEv2 messages. An attacker could exploit this vulnerability by sending crafted IKEv2 traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition on the affected device. | 2025-05-07 | 8.6 |
| CVE-2025-31644 | f5 - BIG-IP | When running in Appliance mode, a command injection vulnerability exists in an undisclosed iControl REST and BIG-IP TMOS Shell (tmsh) command which may allow an authenticated attacker with administrator role privileges to execute arbitrary system commands. 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. | 2025-05-07 | 8.5 |
| CVE-2025-22477 | dell - multiple products | Dell Storage Center - Dell Storage Manager, version(s) 20.1.20, contain(s) an Improper Authentication vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Elevation of privileges. | 2025-05-06 | 8.3 |
| CVE-2025-20164 | cisco - IOS | A vulnerability in the Cisco Industrial Ethernet Switch Device Manager (DM) of Cisco IOS Software could allow an authenticated, remote attacker to elevate privileges. This vulnerability is due to insufficient validation of authorizations for authenticated users. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to elevate privileges to privilege level 15. To exploit this vulnerability, the attacker must have valid credentials for a user account with privilege level 5 or higher. Read-only DM users are assigned privilege level 5. | 2025-05-07 | 8.3 |
| CVE-2025-32820 | sonicwall - SMA100 | A vulnerability in SMA100 allows a remote authenticated attacker with SSLVPN user privileges can inject a path traversal sequence to make any directory on the SMA appliance writable. | 2025-05-07 | 8.3 |
| CVE-2025-43878 | f5 - multiple products | When running in Appliance mode, an authenticated attacker assigned the Administrator or Resource Administrator role may be able to bypass Appliance mode restrictions utilizing system diagnostics tcpdump command utility on a F5OS-C/A system.<br>Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. | 2025-05-07 | 8.3 |
| CVE-2024-49846 | qualcomm - qca6688aq_firmware | Memory corruption while decoding of OTA messages from T3448 IE. | 2025-05-06 | 8.2 |
| CVE-2025-3528 | red hat - mirror registry for Red Hat OpenShift | A flaw was found in the Mirror Registry. The quay-app container shipped as part of the Mirror Registry for OpenShift has write access to the `/etc/passwd`. This flaw allows a malicious actor with access to the container to modify the passwd file and elevate their privileges to the root user within that pod. | 2025-05-09 | 8.2 |
| CVE-2025-22478 | dell - multiple products | Dell Storage Center - Dell Storage Manager, version(s) 20.1.20, contain(s) an Improper Restriction of XML External Entity Reference vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Information disclosure and Information tampering. | 2025-05-06 | 8.1 |
| CVE-2025-33072 | microsoft - Microsoft msagsfeedback.azurewebsites.net | Improper access control in Azure allows an unauthorized attacker to disclose information over a network. | 2025-05-08 | 8.1 |
| CVE-2025-20668 | google - multiple products | In scp, 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: ALPS09625562; Issue ID: MSV-3027. | 2025-05-05 | 7.8 |
| CVE-2025-2509 | google - ChromeOS | Out-of-Bounds Read in Virglrenderer in ChromeOS  16093.57.0 allows a malicious guest VM to achieve arbitrary address access within the crosvm sandboxed process, potentially leading to VM escape via crafted vertex elements data triggering an out-of-bounds read in util_format_description. | 2025-05-06 | 7.8 |
| CVE-2025-46584 | huawei - harmonyos | Vulnerability of improper authentication logic implementation in the file system module<br>Impact: Successful exploitation of this vulnerability may affect service confidentiality. | 2025-05-06 | 7.8 |
| CVE-2024-45554 | qualcomm - fastconnect_6900_firmware | Memory corruption during concurrent SSR execution due to race condition on the global maps list. | 2025-05-06 | 7.8 |
| CVE-2024-45564 | qualcomm - c-v2x_9150_firmware | Memory corruption during concurrent access to server info object due to incorrect reference count update. | 2025-05-06 | 7.8 |
| CVE-2024-45565 | qualcomm - sdm429w_firmware | Memory corruption when blob structure is modified by user-space after kernel verification. | 2025-05-06 | 7.8 |
| CVE-2024-45566 | qualcomm - fastconnect_6800_firmware | Memory corruption during concurrent buffer access due to modification of the reference count. | 2025-05-06 | 7.8 |
| CVE-2024-45567 | qualcomm - fastconnect_6900_firmware | Memory corruption while encoding JPEG format. | 2025-05-06 | 7.8 |
| CVE-2024-45574 | qualcomm - sdm429w_firmware | Memory corruption during array access in Camera kernel due to invalid index from invalid command data. | 2025-05-06 | 7.8 |
| CVE-2024-45575 | qualcomm - fastconnect_6900_firmware | Memory corruption Camera kernel when large number of devices are attached through userspace. | 2025-05-06 | 7.8 |
| CVE-2024-45576 | qualcomm - fastconnect_6900_firmware | Memory corruption while prociesing command buffer buffer in OPE module. | 2025-05-06 | 7.8 |
| CVE-2024-45577 | qualcomm - fastconnect_6900_firmware | Memory corruption while invoking IOCTL calls from userspace to camera kernel driver to dump request information. | 2025-05-06 | 7.8 |

| | | | | |
|---|---|---|---|---|
| CVE-2024-45578 | qualcomm - fastconnect_6900_firmware | Memory corruption while acquire and update IOCTLs during IFE output resource ID validation. | 2025-05-06 | 7.8 |
| CVE-2024-45579 | qualcomm - fastconnect_6900_firmware | Memory corruption may occur when invoking IOCTL calls from userspace to the camera kernel driver to dump request information, due to a missing memory requirement check. | 2025-05-06 | 7.8 |
| CVE-2024-49835 | qualcomm - aqt1000_firmware | Memory corruption while reading secure file. | 2025-05-06 | 7.8 |
| CVE-2024-49841 | qualcomm - snapdragon_ar2_gen_1_firmware | Memory corruption during memory assignment to headless peripheral VM due to incorrect error code handling. | 2025-05-06 | 7.8 |
| CVE-2024-49842 | qualcomm - aqt1000_firmware | Memory corruption during memory mapping into protected VM address space due to incorrect API restrictions. | 2025-05-06 | 7.8 |
| CVE-2024-49844 | qualcomm - ar8035_firmware | Memory corruption while triggering commands in the PlayReady Trusted application. | 2025-05-06 | 7.8 |
| CVE-2024-49845 | qualcomm - wcd9385_firmware | Memory corruption during the FRS UDS generation process. | 2025-05-06 | 7.8 |
| CVE-2025-21453 | qualcomm - 315_5g_iot_modem_firmware | Memory corruption while processing a data structure, when an iterator is accessed after it has been removed, potential failures occur. | 2025-05-06 | 7.8 |
| CVE-2025-21460 | qualcomm - qam8255p_firmware | Memory corruption while processing a message, when the buffer is controlled by a Guest VM, the value can be changed continuously. | 2025-05-06 | 7.8 |
| CVE-2025-21462 | qualcomm - fastconnect_6900_firmware | Memory corruption while processing an IOCTL request, when buffer significantly exceeds the command argument limit. | 2025-05-06 | 7.8 |
| CVE-2025-21467 | qualcomm - csra6620_firmware | Memory corruption while reading the FW response from the shared queue. | 2025-05-06 | 7.8 |
| CVE-2025-21468 | qualcomm - ar8035_firmware | Memory corruption while reading response from FW, when buffer size is changed by FW while driver is using this size to write null character at the end of buffer. | 2025-05-06 | 7.8 |
| CVE-2025-21469 | qualcomm - fastconnect_6700_firmware | Memory corruption while processing image encoding, when input buffer length is 0 in IOCTL call. | 2025-05-06 | 7.8 |
| CVE-2025-21470 | qualcomm - aqt1000_firmware | Memory corruption while processing image encoding, when configuration is NULL in IOCTL parameter. | 2025-05-06 | 7.8 |
| CVE-2025-21475 | qualcomm - aqt1000_firmware | Memory corruption while processing escape code, when DisplayId is passed with large unsigned value. | 2025-05-06 | 7.8 |
| CVE-2025-20122 | cisco - Cisco Catalyst SD-WAN Manager | A vulnerability in the CLI of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, local attacker to gain privileges of the root user on the underlying operating system. This vulnerability is due to insufficient input validation. An authenticated attacker with read-only privileges on the SD-WAN Manager system could exploit this vulnerability by sending a crafted request to the CLI of the SD-WAN Manager. A successful exploit could allow the attacker to gain root privileges on the underlying operating system. | 2025-05-07 | 7.8 |
| CVE-2025-1329 | ibm - multiple products | IBM CICS TX Standard 11.1 and IBM CICS TX Advanced 10.1 and 11.1 could allow a local user to execute arbitrary code on the system due to failure to handle DNS return requests by the gethostbyaddr function. | 2025-05-08 | 7.8 |
| CVE-2025-1330 | ibm - multiple products | IBM CICS TX Standard 11.1 and IBM CICS TX Advanced 10.1 and 11.1  could allow a local user to execute arbitrary code on the system due to failure to handle DNS return requests by the gethostbyname  function. | 2025-05-08 | 7.8 |
| CVE-2025-1331 | ibm - multiple products | IBM CICS TX Standard 11.1 and IBM CICS TX Advanced 10.1 and 11.1 could allow a local user to execute arbitrary code on the system due to the use of unsafe use of the gets function. | 2025-05-08 | 7.8 |
| CVE-2025-20192 | cisco - Cisco IOS XE Software | A vulnerability in the Internet Key Exchange version 1 (IKEv1) implementation of Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The attacker must have valid IKEv1 VPN credentials to exploit this vulnerability. This vulnerability is due to improper validation of IKEv1 phase 2 parameters before the IPsec security association creation request is handed off to the hardware cryptographic accelerator of an affected device. An attacker could exploit this vulnerability by sending crafted IKEv1 messages to the affected device. A successful exploit could allow the attacker to cause the device to reload. | 2025-05-07 | 7.7 |
| CVE-2025-46585 | huawei - harmonyos | Out-of-bounds array read/write vulnerability in the kernel module<br>Impact: Successful exploitation of this vulnerability may affect availability. | 2025-05-06 | 7.5 |
| CVE-2024-49847 | qualcomm - ar8035_firmware | Transient DOS while processing of a registration acceptance OTA due to incorrect ciphering key data IE. | 2025-05-06 | 7.5 |
| CVE-2025-21459 | qualcomm - ar8035_firmware | Transient DOS while parsing per STA profile in ML IE. | 2025-05-06 | 7.5 |
| CVE-2025-2898 | ibm - maximo_application_suite | IBM Maximo Application Suite 9.0 could allow an attacker with some level of access to elevate their privileges due to a security configuration vulnerability in Role-Based Access Control (RBAC) configurations. | 2025-05-06 | 7.5 |
| CVE-2025-33093 | ibm - Sterling Partner Engagement Manager | IBM Sterling Partner Engagement Manager 6.1.0, 6.2.0, 6.2.2 JWT secret is stored in public Helm Charts and is not stored as a Kubernetes secret. | 2025-05-07 | 7.5 |
| CVE-2025-1137 | ibm - Storage Scale | IBM Storage Scale 5.2.2.0 and 5.2.2.1, under certain configurations, could allow an authenticated user to execute privileged commands due to improper input neutralization. | 2025-05-10 | 7.5 |
| CVE-2025-20140 | cisco - Cisco IOS XE Software | A vulnerability in the Wireless Network Control daemon (wncd) of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent wireless attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper memory management. An attacker could exploit this vulnerability by sending a series of IPv6 network | 2025-05-07 | 7.4 |

| | | | | |
|---|---|---|---|---|
| | | requests from an associated wireless IPv6 client to an affected device. To associate a client to a device, an attacker may first need to authenticate to the network, or associate freely in the case of a configured open network. A successful exploit could allow the attacker to cause the wncd process to consume available memory and eventually cause the device to stop responding, resulting in a DoS condition. | | |
| CVE-2025-20189 | cisco - Cisco IOS XE Software | A vulnerability in the Cisco Express Forwarding functionality of Cisco IOS XE Software for Cisco ASR 903 Aggregation Services Routers with Route Switch Processor 3 (RSP3C) could allow an unauthenticated, adjacent attacker to trigger a denial of service (DoS) condition.<br>This vulnerability is due to improper memory management when Cisco IOS XE Software is processing Address Resolution Protocol (ARP) messages. An attacker could exploit this vulnerability by sending crafted ARP messages at a high rate over a period of time to an affected device. A successful exploit could allow the attacker to exhaust system resources, which eventually triggers a reload of the active route switch processor (RSP). If a redundant RSP is not present, the router reloads. | 2025-05-07 | 7.4 |
| CVE-2025-20191 | cisco - multiple products | A vulnerability in the Switch Integrated Security Features (SISF) of Cisco IOS Software, Cisco IOS XE Software, Cisco NX-OS Software, and Cisco Wireless LAN Controller (WLC) AireOS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to the incorrect handling of DHCPv6 packets. An attacker could exploit this vulnerability by sending a crafted DHCPv6 packet to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. | 2025-05-07 | 7.4 |
| CVE-2025-20202 | cisco - Cisco IOS XE Software | A vulnerability in Cisco IOS XE Wireless Controller Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device.<br>This vulnerability is due to insufficient input validation of access point (AP) Cisco Discovery Protocol (CDP) neighbor reports when they are processed by the wireless controller. An attacker could exploit this vulnerability by sending a crafted CDP packet to an AP. A successful exploit could allow the attacker to cause an unexpected reload of the wireless controller that is managing the AP, resulting in a DoS condition that affects the wireless network. | 2025-05-07 | 7.4 |
| CVE-2025-20210 | cisco - Cisco Digital Network Architecture Center (DNA Center) | A vulnerability in the management API of Cisco Catalyst Center, formerly Cisco DNA Center, could allow an unauthenticated, remote attacker to read and modify the outgoing proxy configuration settings. This vulnerability is due to the lack of authentication in an API endpoint. An attacker could exploit this vulnerability by sending a request to the affected API of a Catalyst Center device. A successful exploit could allow the attacker to view or modify the outgoing proxy configuration, which could disrupt internet traffic from Cisco Catalyst Center or may allow the attacker to intercept outbound internet traffic. | 2025-05-07 | 7.3 |
| CVE-2025-46762 | apache - parquet | Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code.<br>While 1.15.1 introduced a fix to restrict untrusted packages, the default setting of trusted packages still allows malicious classes from these packages to be executed.<br>The exploit is only applicable if the client code of parquet-avro uses the "specific" or the "reflect" models deliberately for reading Parquet files. ("generic" model is not impacted)<br>Users are recommended to upgrade to 1.15.2 or set the system property "org.apache.parquet.avro.SERIALIZABLE_PACKAGES" to an empty string on 1.15.1. Both are sufficient to fix the issue. | 2025-05-06 | 7.1 |
| CVE-2025-32821 | sonicwall - SMA100 | A vulnerability in SMA100 allows a remote authenticated attacker with SSLVPN admin privileges can with admin privileges can inject shell command arguments to upload a file on the appliance. | 2025-05-07 | 7.1 |
| CVE-2025-20671 | google - multiple products | In thermal, there is a possible out of bounds write due to a race condition. 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: ALPS09698599; Issue ID: MSV-3228. | 2025-05-05 | 7 |
| CVE-2025-4388 | liferay - multiple products | A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.5, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12, 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the modules/apps/marketplace/marketplace-app-manager-web. | 2025-05-06 | 6.9 |
| CVE-2025-27533 | apache software foundation - Apache ActiveMQ | Memory Allocation with Excessive Size Value vulnerability in Apache ActiveMQ.<br>During unmarshalling of OpenWire commands the size value of buffers was not properly validated which could lead to excessive memory allocation and be exploited to cause a denial of service (DoS) by depleting process memory, thereby affecting applications and services that rely on the availability of the ActiveMQ broker when not using mutual TLS connections.<br>This issue affects Apache ActiveMQ: from 6.0.0 before 6.1.6, from 5.18.0 before 5.18.7, from 5.17.0 before 5.17.7, before 5.16.8. ActiveMQ 5.19.0 is not affected.<br>Users are recommended to upgrade to version 6.1.6+, 5.19.0+, 5.18.7+, 5.17.7, or 5.16.8 or which fixes the issue.<br>Existing users may implement mutual TLS to mitigate the risk on affected brokers. | 2025-05-07 | 6.9 |
| CVE-2025-20181 | cisco - IOS | A vulnerability in Cisco IOS Software for Cisco Catalyst 2960X, 2960XR, 2960CX, and 3560CX Series Switches could allow an authenticated, local attacker with privilege level 15 or an unauthenticated attacker with physical access to the device to execute persistent code at boot time and break the chain of trust. This vulnerability is due to missing signature verification for specific files that may be loaded during the device boot process. An attacker could exploit this vulnerability by placing a crafted file into a specific location on an affected device. A successful exploit could allow the attacker to execute arbitrary code at boot time. Because this allows the attacker to bypass a major security feature of the device, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High. | 2025-05-07 | 6.8 |
| CVE-2024-45568 | qualcomm - fastconnect_6900_firmware | Memory corruption due to improper bounds check while command handling in camera-kernel driver. | 2025-05-06 | 6.7 |
| CVE-2024-49829 | qualcomm - fastconnect_6900_firmware | Memory corruption can occur during context user dumps due to inadequate checks on buffer length. | 2025-05-06 | 6.7 |

| | | | | |
|---|---|---|---|---|
| CVE-2025-20937 | samsung - multiple products | Out-of-bounds write in Keymaster trustlet prior to SMR May-2025 Release 1 allows local privileged attackers to write out-of-bounds memory. | 2025-05-07 | 6.7 |
| CVE-2025-20197 | cisco - Cisco IOS XE Software | A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation when processing specific configuration commands. An attacker could exploit this vulnerability by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The security impact rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15. | 2025-05-07 | 6.7 |
| CVE-2025-20200 | cisco - Cisco IOS XE Software | A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation when processing specific configuration commands. An attacker could exploit this vulnerability by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The security impact rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15. | 2025-05-07 | 6.7 |
| CVE-2025-20201 | cisco - Cisco IOS XE Software | A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation when processing specific configuration commands. An attacker could exploit this vulnerability by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The security impact rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions.<br>Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15. | 2025-05-07 | 6.7 |
| CVE-2024-45562 | qualcomm - c-v2x_9150_firmware | Memory corruption during concurrent access to server info object due to unprotected critical field. | 2025-05-06 | 6.6 |
| CVE-2024-45563 | qualcomm - fastconnect_6900_firmware | Memory corruption while handling schedule request in Camera Request Manager(CRM) due to invalid link count in the corresponding session. | 2025-05-06 | 6.6 |
| CVE-2024-45570 | qualcomm - qca6391_firmware | Memory corruption may occur during IO configuration processing when the IO port count is invalid. | 2025-05-06 | 6.6 |
| CVE-2024-45581 | qualcomm - mdm9628_firmware | Memory corruption while sound model registration for voice activation with audio kernel driver. | 2025-05-06 | 6.6 |
| CVE-2024-45583 | qualcomm - fastconnect_7800_firmware | Memory corruption while handling multiple IOCTL calls from userspace to operate DMA operations. | 2025-05-06 | 6.6 |
| CVE-2024-49830 | qualcomm - qca6574au_firmware | Memory corruption while processing an IOCTL call to set mixer controls. | 2025-05-06 | 6.6 |
| CVE-2025-4374 | red hat - Red Hat Quay 3 | A flaw was found in Quay. When an organization acts as a proxy cache, and a user or robot pulls an image that hasn't been mirrored yet, they are granted "Admin" permissions on the newly created repository. | 2025-05-06 | 6.5 |
| CVE-2025-20187 | cisco - Cisco Catalyst SD-WAN Manager | A vulnerability in the application data endpoints of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, remote attacker to write arbitrary files to an affected system. This vulnerability is due to improper validation of requests to APIs. An attacker could exploit this vulnerability by sending malicious requests to an API within the affected system. A successful exploit could allow the attacker to conduct directory traversal attacks and write files to an arbitrary location on the affected system. | 2025-05-07 | 6.5 |
| CVE-2025-20190 | cisco - Cisco IOS XE Software | A vulnerability in the lobby ambassador web interface of Cisco IOS XE Wireless Controller Software could allow an authenticated, remote attacker to remove arbitrary users that are defined on an affected device. This vulnerability is due to insufficient access control of actions executed by lobby ambassador users. An attacker could exploit this vulnerability by logging in to an affected device with a lobby ambassador user account and sending crafted HTTP requests to the API. A successful exploit could allow the attacker to delete arbitrary user accounts on the device, including users with administrative privileges. Note: This vulnerability is exploitable only if the attacker obtains the credentials for a lobby ambassador account. This account is not configured by default. | 2025-05-07 | 6.5 |
| CVE-2025-20193 | cisco - Cisco IOS XE Software | A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, low-privileged, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface. A successful exploit could allow the attacker to read files from the underlying operating system. | 2025-05-07 | 6.5 |
| CVE-2025-46392 | apache software foundation - Apache Commons Configuration | Uncontrolled Resource Consumption vulnerability in Apache Commons Configuration 1.x.<br>There are a number of issues in Apache Commons Configuration 1.x that allow excessive resource consumption when loading untrusted configurations or using unexpected usage patterns. The Apache Commons Configuration team does not intend to fix these issues in 1.x. Apache Commons Configuration 1.x is still safe to use in scenario's where you only load trusted configurations.<br>Users that load untrusted configurations or give attackers control over usage patterns are recommended to upgrade to the 2.x version line, which fixes these issues. Apache Commons | 2025-05-09 | 6.5 |

| | | | | |
|---|---|---|---|---|
| | | Configuration 2.x is not a drop-in replacement, but as it uses a separate Maven groupId and Java package namespace they can be loaded side-by-side, making it possible to do a gradual migration. | | |
| CVE-2025-4051 | google - Chrome | Insufficient data validation in DevTools in Google Chrome prior to 136.0.7103.59 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium) | 2025-05-05 | 6.3 |
| CVE-2025-46590 | huawei - harmonyos | Bypass vulnerability in the network search instruction authentication module<br>Impact: Successful exploitation of this vulnerability can bypass authentication and enable access to some network search functions. | 2025-05-06 | 6.3 |
| CVE-2024-58252 | huawei - harmonyos | Vulnerability of insufficient information protection in the media library module<br>Impact: Successful exploitation of this vulnerability may affect service confidentiality. | 2025-05-06 | 6.2 |
| CVE-2025-46587 | huawei - harmonyos | Permission control vulnerability in the media library module<br>Impact: Successful exploitation of this vulnerability may affect service confidentiality. | 2025-05-06 | 6.2 |
| CVE-2025-46591 | huawei - harmonyos | Out-of-bounds data read vulnerability in the authorization module<br>Impact: Successful exploitation of this vulnerability may affect service confidentiality. | 2025-05-06 | 6.2 |
| CVE-2025-20155 | cisco - Cisco IOS XE Software | A vulnerability in the bootstrap loading of Cisco IOS XE Software could allow an authenticated, local attacker to write arbitrary files to an affected system.<br>This vulnerability is due to insufficient input validation of the bootstrap file that is read by the system software when a device is first deployed in SD-WAN mode or when an administrator configures SD-Routing on the device. An attacker could exploit this vulnerability by modifying a bootstrap file generated by Cisco Catalyst SD-WAN Manager, loading it into the device flash, and then either reloading the device in a green field deployment in SD-WAN mode or configuring the device with SD-Routing. A successful exploit could allow the attacker to perform arbitrary file writes to the underlying operating system. | 2025-05-07 | 6.0 |
| CVE-2025-20157 | cisco - Cisco Catalyst SD-WAN Manager | A vulnerability in certificate validation processing of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an unauthenticated, remote attacker to gain access to sensitive information. This vulnerability is due to improper validation of certificates that are used by the Smart Licensing feature. An attacker with a privileged network position could exploit this vulnerability by intercepting traffic that is sent over the Internet. A successful exploit could allow the attacker to gain access to sensitive information, including credentials used by the device to connect to Cisco cloud services. | 2025-05-07 | 5.9 |
| CVE-2025-4382 | red hat - multiple products | A flaw was found in systems utilizing LUKS-encrypted disks with GRUB configured for TPM-based auto-decryption. When GRUB is set to automatically decrypt disks using keys stored in the TPM, it reads the decryption key into system memory. If an attacker with physical access can corrupt the underlying filesystem superblock, GRUB will fail to locate a valid filesystem and enter rescue mode. At this point, the disk is already decrypted, and the decryption key remains loaded in system memory. This scenario may allow an attacker with physical access to access the unencrypted data without any further authentication, thereby compromising data confidentiality. Furthermore, the ability to force this state through filesystem corruption also presents a data integrity concern. | 2025-05-09 | 5.9 |
| CVE-2025-20665 | google - multiple products | In devinfo, there is a possible information disclosure due to a missing SELinux policy. This could lead to local information disclosure of device identifier with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09555228; Issue ID: MSV-2760. | 2025-05-05 | 5.5 |
| CVE-2025-22476 | dell - Dell Storage Center - Dell Storage Manager | Dell Storage Center - Dell Storage Manager, version(s) 20.1.20, contain(s) an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Remote execution. | 2025-05-06 | 5.5 |
| CVE-2025-20954 | samsung - multiple products | Use of implicit intent for sensitive communication in EnrichedCall prior to SMR May-2025 Release 1 allows local attackers to access sensitive information. User interaction is required for triggering this vulnerability. | 2025-05-07 | 5.5 |
| CVE-2025-20213 | cisco - Cisco Catalyst SD-WAN Manager | A vulnerability in the CLI of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. To exploit this vulnerability, the attacker must have valid read-only credentials with CLI access on the affected system. This vulnerability is due to improper access controls on files that are on the local file system. An attacker could exploit this vulnerability by running a series of crafted commands on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device and gain privileges of the root user. To exploit this vulnerability, an attacker would need to have CLI access as a low-privilege user. | 2025-05-07 | 5.5 |
| CVE-2025-30102 | dell - powerscale_onefs | Dell PowerScale OneFS, versions 9.4.0.0 through 9.10.1.0, contains an out-of-bounds write vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to denial of service. | 2025-05-08 | 5.5 |
| CVE-2025-3218 | ibm - i | IBM i 7.2, 7.3, 7.4, 7.5, and 7.6 is vulnerable to authentication and authorization attacks due to incorrect validation processing in IBM i Netserver. A malicious actor could use the weaknesses, in conjunction with brute force authentication attacks or to bypass authority restrictions, to access the server. | 2025-05-07 | 5.4 |
| CVE-2025-20147 | cisco - Cisco Catalyst SD-WAN Manager | A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, remote attacker to conduct a stored cross-site scripting attack (XSS) on an affected system.&nbsp; This vulnerability is due to improper sanitization of user input to the web-based management interface. An attacker could exploit this vulnerability by submitting a malicious script through the interface. A successful exploit could allow the attacker to conduct a stored XSS attack on the affected system. | 2025-05-07 | 5.4 |
| CVE-2025-20194 | cisco - Cisco IOS XE Software | A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, low-privileged, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface. A successful exploit could allow the attacker to read limited files from the underlying operating system or clear the syslog and licensing logs on the affected device. | 2025-05-07 | 5.4 |
| CVE-2025-1992 | ibm - Db2 for Linux, UNIX and Windows | IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.1 could allow an authenticated user, under non default configurations, to cause a denial of service due to insufficient release of allocated memory after usage. | 2025-05-05 | 5.3 |

| | | | | |
|---|---|---|---|---|
| CVE-2025-0915 | ibm - multiple products | IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.1 under specific configurations could allow an authenticated user to cause a denial of service due to insufficient release of allocated memory resources. | 2025-05-05 | 5.3 |
| CVE-2025-1000 | ibm - multiple products | IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5.0 through 11.5.9 and 12.1.0 through 12.1.1 could allow an authenticated user to cause a denial of service when connecting to a z/OS database due to improper handling of automatic client rerouting. | 2025-05-05 | 5.3 |
| CVE-2025-1493 | ibm - multiple products | IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) 12.1.0 through 12.1.1 could allow an authenticated user to cause a denial of service due to concurrent execution of shared resources. | 2025-05-05 | 5.3 |
| CVE-2025-20196 | cisco - multiple products | A vulnerability in the Cisco IOx application hosting environment of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the Cisco IOx application hosting environment to stop responding, resulting in a denial of service (DoS) condition.<br>This vulnerability is due to the improper handling of HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to cause the Cisco IOx application hosting environment to stop responding. The IOx process will need to be manually restarted to recover services. | 2025-05-07 | 5.3 |
| CVE-2025-20221 | cisco - Cisco IOS XE Software | A vulnerability in the packet filtering features of Cisco IOS XE SD-WAN Software could allow an unauthenticated, remote attacker to bypass Layer 3 and Layer 4 traffic filters.<br>This vulnerability is due to improper traffic filtering conditions on an affected device. An attacker could exploit this vulnerability by sending a crafted packet to the affected device. A successful exploit could allow the attacker to bypass the Layer 3 and Layer 4 traffic filters and inject a crafted packet into the network. | 2025-05-07 | 5.3 |
| CVE-2025-4432 | red hat - multiple products | A flaw was found in Rust's Ring package. A panic may be triggered when overflow checking is enabled. In the QUIC protocol, this flaw allows an attacker to induce this panic by sending a specially crafted packet. It will likely occur unintentionally in 1 out of every 2**32 packets sent or received. | 2025-05-09 | 5.3 |
| CVE-2025-46586 | huawei - harmonyos | Permission control vulnerability in the contacts module<br>Impact: Successful exploitation of this vulnerability may affect availability. | 2025-05-06 | 5.1 |
| CVE-2025-46593 | huawei - harmonyos | Process residence vulnerability in abnormal scenarios in the print module<br>Impact: Successful exploitation of this vulnerability may affect availability. | 2025-05-06 | 5.1 |
| CVE-2025-20953 | samsung - multiple products | Improper access control in SmartManagerCN prior to SMR May-2025 Release 1 allows local attackers to launch activities within SmartManagerCN. | 2025-05-07 | 5.1 |
| CVE-2025-1993 | ibm - App Connect Enterprise Certified Container | IBM App Connect Enterprise Certified Container 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, and 12.10 DesignerAuthoring instances store their flows in a database that is protected by weaker than expected cryptographic algorithms that could be decrypted by a local user. | 2025-05-09 | 5.1 |
| CVE-2025-27695 | dell - Wyse Management Suite | Dell Wyse Management Suite, versions prior to WMS 5.1 contain an Authentication Bypass by Spoofing vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information Disclosure. | 2025-05-08 | 4.9 |
| CVE-2025-4373 | red hat - multiple products | A flaw was found in GLib, which is vulnerable to an integer overflow in the g_string_insert_unichar() function. When the position at which to insert the character is large, the position will overflow, leading to a buffer underwrite. | 2025-05-06 | 4.8 |
| CVE-2025-20137 | cisco - IOS | A vulnerability in the access control list (ACL) programming of Cisco IOS Software that is running on Cisco Catalyst 1000 Switches and Cisco Catalyst 2960L Switches could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to the use of both an IPv4 ACL and a dynamic ACL of IP Source Guard on the same interface, which is an unsupported configuration. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device. Note: Cisco documentation has been updated to reflect that this is an unsupported configuration. However, Cisco is publishing this advisory because the device will not prevent an administrator from configuring both features on the same interface. There are no plans to implement the ability to configure both features on the same interface on Cisco Catalyst 1000 or Catalyst 2960L Switches. | 2025-05-07 | 4.7 |
| CVE-2025-20216 | cisco - Cisco Catalyst SD-WAN Manager | A vulnerability in the web interface of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an unauthenticated, remote attacker to inject HTML into the browser of an authenticated user.<br>This vulnerability is due to improper sanitization of input to the web interface. An attacker could exploit this vulnerability by convincing an authenticated user to click a malicious link. A successful exploit could allow the attacker to inject HTML into the browser of an authenticated Cisco Catalyst SD-WAN Manager user. | 2025-05-07 | 4.7 |
| CVE-2025-20223 | cisco - Cisco Digital Network Architecture Center (DNA Center) | A vulnerability in Cisco Catalyst Center, formerly Cisco DNA Center, could allow an authenticated, remote attacker to read and modify data in a repository that belongs to an internal service of an affected device. This vulnerability is due to insufficient enforcement of access control on HTTP requests. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device. | 2025-05-07 | 4.7 |
| CVE-2025-20198 | cisco - Cisco IOS XE Software | A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation when processing specific configuration commands. An attacker could exploit this vulnerability by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The security impact rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15. | 2025-05-07 | 4.6 |
| CVE-2025-20199 | cisco - Cisco IOS XE Software | A vulnerability in the CLI of Cisco IOS XE Software could allow an authenticated, local attacker with privilege level 15 to elevate privileges to root on the underlying operating system of an affected device. This vulnerability is due to insufficient input validation when processing specific | 2025-05-07 | 4.6 |

| | | | | |
|---|---|---|---|---|
| | | configuration commands. An attacker could exploit this vulnerability by including crafted input in specific configuration commands. A successful exploit could allow the attacker to elevate privileges to root on the underlying operating system of an affected device. The security impact rating (SIR) of this advisory has been raised to High because an attacker could gain access to the underlying operating system of the affected device and perform potentially undetected actions. Note: The attacker must have privileges to enter configuration mode on the affected device. This is usually referred to as privilege level 15. | | |
| CVE-2025-47814 | gnu - PSPP | libpspp-core.a in GNU PSPP through 2.0.1 allows attackers to cause a heap-based buffer overflow in inflate_read (called indirectly from spv_read_xml_member) in zip-reader.c. | 2025-05-10 | 4.5 |
| CVE-2025-47815 | gnu - PSPP | libpspp-core.a in GNU PSPP through 2.0.1 allows attackers to cause a heap-based buffer overflow in inflate_read (called indirectly from zip_member_read_all) in zip-reader.c. | 2025-05-10 | 4.5 |
| CVE-2025-46588 | huawei - harmonyos | Vulnerability of unauthorized access in the app lock module<br>Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. | 2025-05-06 | 4.4 |
| CVE-2025-46589 | huawei - harmonyos | Vulnerability of unauthorized access in the app lock module<br>Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. | 2025-05-06 | 4.4 |
| CVE-2025-46592 | huawei - harmonyos | Null pointer dereference vulnerability in the USB HDI driver module<br>Impact: Successful exploitation of this vulnerability may affect availability. | 2025-05-06 | 4.4 |
| CVE-2025-30101 | dell - powerscale_onefs | Dell PowerScale OneFS, versions 9.8.0.0 through 9.10.1.0, contain a time-of-check time-of-use (TOCTOU) race condition vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to denial of service and information tampering. | 2025-05-08 | 4.4 |
| CVE-2025-20151 | cisco - Cisco IOS XE Catalyst SD-WAN | A vulnerability in the implementation of the Simple Network Management Protocol Version 3 (SNMPv3) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to poll an affected device using SNMP, even if the device is configured to deny SNMP traffic from an unauthorized source or the SNMPv3 username is removed from the configuration.<br>This vulnerability exists because of the way that the SNMPv3 configuration is stored in the Cisco IOS Software and Cisco IOS XE Software startup configuration. An attacker could exploit this vulnerability by polling an affected device from a source address that should have been denied. A successful exploit could allow the attacker to perform SNMP operations from a source that should be denied.<br>Note: The attacker has no control of the SNMPv3 configuration. To exploit this vulnerability, the attacker must have valid SNMPv3 user credentials.<br>For more information, see the  section of this advisory. | 2025-05-07 | 4.3 |
| CVE-2025-20195 | cisco - Cisco IOS XE Software | A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a CSRF attack and execute commands on the CLI of an affected device.<br>This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an already authenticated user to follow a crafted link. A successful exploit could allow the attacker to clear the syslog, parser, and licensing logs on the affected device if the targeted user has privileges to clear those logs. | 2025-05-07 | 4.3 |
| CVE-2025-20214 | cisco - Cisco IOS XE Software | A vulnerability in the Network Configuration Access Control Module (NACM) of Cisco IOS XE Software could allow an authenticated, remote attacker to obtain unauthorized read access to configuration or operational data.<br>This vulnerability exists because a subtle change in inner API call behavior causes results to be filtered incorrectly. An attacker could exploit this vulnerability by using either NETCONF, RESTCONF, or gRPC Network Management Interface (gNMI) protocols and query data on paths that may have been denied by the NACM configuration. A successful exploit could allow the attacker to access data that should have been restricted according to the NACM configuration.<br>Note: This vulnerability requires that the attacker obtain the credentials from a valid user with privileges lower than 15, and that NACM was configured to provide restricted read access for that user. | 2025-05-07 | 4.3 |
| CVE-2025-22479 | dell - multiple products | Dell Storage Center - Dell Storage Manager, version(s) 20.0.21, contain(s) an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Script injection. | 2025-05-06 | 3.5 |
| CVE-2025-23379 | dell - multiple products | Dell Storage Center - Dell Storage Manager, version(s) 21.0.20, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Script injection. | 2025-05-06 | 3.5 |
| CVE-2025-47816 | gnu - PSPP | libpspp-core.a in GNU PSPP through 2.0.1 allows attackers to cause an spvxml-helpers.c spvxml_parse_attributes out-of-bounds read, related to extra content at the end of a document. | 2025-05-10 | 2.9 |

**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.**