الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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 ١٠ أغسطس إلى ١٦ أغسطس. 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

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 10th of August to 16th of August. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-20265	cisco - multiple products	A vulnerability in the RADIUS subsystem implementation of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to inject arbitrary shell commands that are executed by the device. _x000D_ This vulnerability is due to a lack of proper handling of user input during the authentication phase. An attacker could exploit this vulnerability by sending crafted input when entering credentials that will be authenticated at the configured RADIUS server. A successful exploit could allow the attacker to execute commands at a high privilege level. Note: For this vulnerability to be exploited, Cisco Secure FMC Software must be configured for RADIUS authentication for the web-based management interface, SSH management, or both.	2025-08-14	10
CVE-2025-50165	microsoft - multiple products	Untrusted pointer dereference in Microsoft Graphics Component allows an unauthorized attacker to execute code over a network.	2025-08-12	9.8
CVE-2025-53766	microsoft - multiple products	Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code over a network.	2025-08-12	9.8
CVE-2025-25256	fortinet - multiple products	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiSIEM version 7.3.0 through 7.3.1, 7.2.0 through 7.2.5, 7.1.0 through 7.1.7, 7.0.0 through 7.0.3 and before 6.7.9 allows an unauthenticated attacker to execute unauthorized code or commands via crafted CLI requests.	2025-08-12	9.8
CVE-2025-54466	apache - ofbiz	Improper Control of Generation of Code ('Code Injection') vulnerability leading to a possible RCE in Apache OFBiz scrum plugin. This issue affects Apache OFBiz: before 24.09.02 only when the scrum plugin is used. Even unauthenticated attackers can exploit this vulnerability. Users are recommended to upgrade to version 24.09.02, which fixes the issue.	2025-08-15	9.8
CVE-2025-40746	siemens - simatic_rtls_locating_manager	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.2). Affected products do not properly validate input for a backup script. This could allow an authenticated remote attacker with high privileges in the application to execute arbitrary code with 'NT Authority/SYSTEM' privileges.	2025-08-12	9.4
CVE-2025-50171	microsoft - multiple products	Missing authorization in Remote Desktop Server allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	9.1
CVE-2025-40767	siemens - sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application runs docker containers without adequate security controls to enforce isolation. This could allow an attacker to gain elevated access, potentially accessing sensitive host system resources.	2025-08-12	8.8
CVE-2025-24999	microsoft - multiple products	Improper access control in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-08-12	8.8
CVE-2025-47954	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-08-12	8.8
CVE-2025-49712	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-49757	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	2025-08-12	8.8

CVE-2025-49758	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-08-12	8.8
CVE-2025-49759	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-08-12	8.8
CVE-2025-50163	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-53131	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-53143	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Message Queuing allows an authorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-53144	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Message Queuing allows an authorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-53145	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Message Queuing allows an authorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-53727	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-08-12	8.8
CVE-2025-53772	microsoft - web_deploy_4.0	Deserialization of untrusted data in Web Deploy allows an authorized attacker to execute code over a network.	2025-08-12	8.8
CVE-2025-53778	microsoft - multiple products	Improper authentication in Windows NTLM allows an authorized attacker to elevate privileges over a network.	2025-08-12	8.8
CVE-2025-8879	google - chrome	Heap buffer overflow in libaom in Google Chrome prior to 139.0.7258.127 allowed a remote attacker to potentially exploit heap corruption via a curated set of gestures. (Chromium security severity: High)	2025-08-13	8.8
CVE-2025-8880	google - chrome	Race in V8 in Google Chrome prior to 139.0.7258.127 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2025-08-13	8.8
CVE-2025-8882	google - chrome	Use after free in Aura in Google Chrome prior to 139.0.7258.127 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)	2025-08-13	8.8
CVE-2025-8901	google - chrome	Out of bounds write in ANGLE in Google Chrome prior to 139.0.7258.127 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2025-08-13	8.8
CVE-2025-54809	f5 - F5 Access	F5 Access for Android before version 3.1.2 which uses HTTPS does not verify the remote endpoint identity. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-08-13	8.8
CVE-2024-52504	siemens - multiple products	A vulnerability has been identified in SIPROTEC 4 6MD61 (All versions), SIPROTEC 4 6MD63 (All versions), SIPROTEC 4 6MD66 (All versions), SIPROTEC 4 6MD665 (All versions), SIPROTEC 4 7SA522 (All versions), SIPROTEC 4 7SA6 (All versions < V4.78), SIPROTEC 4 7SD5 (All versions < V4.78), SIPROTEC 4 7SD610 (All versions < V4.78), SIPROTEC 4 7SJ61 (All versions), SIPROTEC 4 7SJ62 (All versions), SIPROTEC 4 7SJ63 (All versions), SIPROTEC 4 7SJ64 (All versions), SIPROTEC 4 7SJ66 (All versions), SIPROTEC 4 7SS52 (All versions), SIPROTEC 4 7ST6 (All versions), SIPROTEC 4 7UM61 (All versions), SIPROTEC 4 7UM62 (All versions), SIPROTEC 4 7UT612 (All versions), SIPROTEC 4 7UT613 (All versions), SIPROTEC 4 7UT63 (All versions), SIPROTEC 4 7VE6 (All versions), SIPROTEC 4 7VK61 (All versions), SIPROTEC 4 7VU683 (All versions), SIPROTEC 4 Compact 7RW80 (All versions), SIPROTEC 4 Compact 7SD80 (All versions), SIPROTEC 4 Compact 7SJ80 (All versions), SIPROTEC 4 Compact 7SJ81 (All versions), SIPROTEC 4 Compact 7SK80 (All versions), SIPROTEC 4 Compact 7SK81 (All versions). Affected devices do not properly handle interrupted operations of file transfer. This could allow an unauthenticated remote attacker to cause a denial of service condition. To restore normal operations, the devices need to be restarted.	2025-08-12	8.7
CVE-2025-40743	siemens - multiple products	A vulnerability has been identified in SINUMERIK 828D PPU.4 (All versions < V4.95 SP5), SINUMERIK 828D PPU.5 (All versions < V5.25 SP1), SINUMERIK 840D sl (All versions < V4.95 SP5), SINUMERIK MC (All versions < V1.25 SP1), SINUMERIK MC V1.15 (All versions < V1.15 SP5), SINUMERIK ONE (All versions < V6.25 SP1), SINUMERIK ONE V6.15 (All versions < V6.15 SP5). The affected application improperly validates authentication for its VNC access service, allowing access with insufficient password verification._x000D_ This could allow an attacker to gain unauthorized remote access and potentially compromise system confidentiality, integrity, or availability.	2025-08-12	8.7
CVE-2025-49557	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be exploited by a low-privileged attacker to inject malicious scripts into vulnerable form fields. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field. Scope is changed.	2025-08-12	8.7
CVE-2025-46405	f5 - BIG-IP	When Network Access is configured on a BIG-IP APM 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.	2025-08-13	8.7
CVE-2025-52585	f5 - BIG-IP	When a BIG-IP LTM Client SSL profile is configured on a virtual server with SSL Forward Proxy enabled and Anonymous Diffie-Hellman (ADH) ciphers enabled, 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.	2025-08-13	8.7
CVE-2025-40758	siemens - multiple products	A vulnerability has been identified in Mendix SAML (Mendix 10.12 compatible) (All versions < V4.0.3), Mendix SAML (Mendix 10.21 compatible) (All versions < V4.1.2), Mendix SAML (Mendix 9.24 compatible) (All versions < V3.6.21). Affected versions of the module insufficiently enforce	2025-08-14	8.7

		signature validation and binding checks. This could allow unauthenticated remote attackers to hijack an account in specific SSO configurations.		
CVE-2024-54678	siemens - multiple products	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), SIMATIC PCS neo V6.0 (All versions), SIMATIC S7-PLCSIM V17 (All versions), SIMATIC STEP 7 V17 (All versions), SIMATIC STEP 7 V18 (All versions), SIMATIC STEP 7 V19 (All versions < V19 Update 4), SIMATIC STEP 7 V20 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V18 (All versions), SIMATIC WinCC V19 (All versions < V19 Update 4), SIMATIC WinCC V20 (All versions), SIMOCODE ES V17 (All versions), SIMOCODE ES V18 (All versions), SIMOCODE ES V19 (All versions), SIMOCODE ES V20 (All versions), SIMOTION SCOUT TIA V5.4 (All versions), SIMOTION SCOUT TIA V5.5 (All versions), SIMOTION SCOUT TIA V5.6 (All versions < V5.6 SP1 HF7), SIMOTION SCOUT TIA V5.7 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SINAMICS Startdrive V19 (All versions), SINAMICS Startdrive V20 (All versions), SIRIUS Safety ES V17 (TIA Portal) (All versions), SIRIUS Safety ES V18 (TIA Portal) (All versions), SIRIUS Safety ES V19 (TIA Portal) (All versions), SIRIUS Safety ES V20 (TIA Portal) (All versions), SIRIUS Soft Starter ES V17 (TIA Portal) (All versions), SIRIUS Soft Starter ES V18 (TIA Portal) (All versions), SIRIUS Soft Starter ES V19 (TIA Portal) (All versions), SIRIUS Soft Starter ES V20 (TIA Portal) (All versions), TIA Portal Cloud V17 (All versions), TIA Portal Cloud V18 (All versions), TIA Portal Cloud V19 (All versions < V5.2.1.1), TIA Portal Cloud V20 (All versions), TIA Portal Test Suite V20 (All versions). Affected products do not properly sanitize Interprocess Communication input received through a Windows Named Pipe accessible to all local users. This could allow an authenticated local attacker to cause a type confusion and execute arbitrary code within the affected application.	2025-08-12	8.6
CVE-2025-40761	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions), RUGGEDCOM ROX MX5000RE (All versions), RUGGEDCOM ROX RX1400 (All versions), RUGGEDCOM ROX RX1500 (All versions), RUGGEDCOM ROX RX1501 (All versions), RUGGEDCOM ROX RX1510 (All versions), RUGGEDCOM ROX RX1511 (All versions), RUGGEDCOM ROX RX1512 (All versions), RUGGEDCOM ROX RX1524 (All versions), RUGGEDCOM ROX RX1536 (All versions), RUGGEDCOM ROX RX5000 (All versions). Affected devices do not properly limit access through its Built-In-Self-Test (BIST) mode. This could allow an attacker with physical access to the serial interface to bypass authentication and get access to a root shell on the device.	2025-08-12	8.6
CVE-2025-20133	cisco - multiple products	A vulnerability in the management and VPN web servers of the Remote Access SSL VPN feature of Cisco Secure Firewall ASA Software and Secure FTD Software could allow an unauthenticated, remote attacker to cause the device to unexpectedly stop responding, resulting in a DoS condition._ This vulnerability is due to ineffective validation of user-supplied input during the Remote Access SSL VPN authentication process. An attacker could exploit this vulnerability by sending a crafted request to the VPN service on an affected device. A successful exploit could allow the attacker to cause a DoS condition where the device stops responding to Remote Access SSL VPN authentication requests.	2025-08-14	8.6
CVE-2025-20134	cisco - multiple products	A vulnerability in the certificate processing of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper parsing of SSL/TLS certificates. An attacker could exploit this vulnerability by sending crafted DNS packets that match a static Network Address Translation (NAT) rule with DNS inspection enabled through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	2025-08-14	8.6
CVE-2025-20136	cisco - multiple products	A vulnerability in the function that performs IPv4 and IPv6 Network Address Translation (NAT) DNS inspection for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. _x000D_ _x000D_ This vulnerability is due to an infinite loop condition that occurs when a Cisco Secure ASA or Cisco Secure FTD device processes DNS packets with DNS inspection enabled and the device is configured for NAT44, NAT64, or NAT46. An attacker could exploit this vulnerability by sending crafted DNS packets that match a static NAT rule with DNS inspection enabled through an affected device. A successful exploit could allow the attacker to create an infinite loop and cause the device to reload, resulting in a DoS condition.	2025-08-14	8.6
CVE-2025-20217	cisco - Cisco Firepower Threat Defense Software	A vulnerability in the packet inspection functionality of the Snort 3 Detection Engine of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device._x000D_ _x000D_ This vulnerability is due to incorrect processing of traffic that is inspected by an affected device. An attacker could exploit this vulnerability by sending crafted traffic through the affected device. A successful exploit could allow the attacker to cause the affected device to enter an infinite loop while inspecting traffic, resulting in a DoS condition. The system watchdog will restart the Snort process automatically.	2025-08-14	8.6
CVE-2025-20222	cisco - Cisco Firepower Threat Defense Software	A vulnerability in the RADIUS proxy feature for the IPsec VPN feature of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to improper processing of IPv6 packets. An attacker could exploit this vulnerability by sending IPv6 packets over an IPsec VPN connection to an affected device. A successful exploit could allow the attacker to trigger a reload of the device, resulting in a DoS condition.	2025-08-14	8.6
CVE-2025-20239	cisco - multiple products	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco IOS Software, IOS XE Software, Secure Firewall Adaptive Security Appliance (ASA) Software, and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition._x000D_	2025-08-14	8.6

		_x000D_ This vulnerability is due to a lack of proper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. In the case of Cisco IOS and IOS XE Software, a successful exploit could allow the attacker to cause the device to reload unexpectedly. In the case of Cisco ASA and FTD Software, a successful exploit could allow the attacker to partially exhaust system memory, causing system instability such as being unable to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.		
CVE-2025-20243	cisco - multiple products	A vulnerability in the management and VPN web servers of Cisco Secure Firewall ASA Software and Secure FTD Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a DoS condition._x000D_ _x000D_ This vulnerability is due to improper validation of user-supplied input on an interface with VPN web services. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted web server on an affected device. A successful exploit could allow the attacker to cause a DoS condition when the device reloads.	2025-08-14	8.6
CVE-2025-20253	cisco - multiple products	A vulnerability in the IKEv2 feature of Cisco IOS Software, IOS XE Software, Secure Firewall ASA Software, and Secure FTD Software could allow an unauthenticated, remote attacker to cause the device to reload, resulting in a DoS condition._x000D_ _x000D_ This vulnerability is due to the improper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to cause an infinite loop that exhausts resources and could cause the device to reload.	2025-08-14	8.6
CVE-2025-20263	cisco - multiple products	A vulnerability in the web services interface of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected system. _x000D_ _x000D_ This vulnerability is due to insufficient boundary checks for specific data that is provided to the web services interface of an affected system. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system, which could cause the system to reload, resulting in a denial of service (DoS) condition.	2025-08-14	8.6
CVE-2025-30033	siemens - multiple products	The affected setup component is vulnerable to DLL hijacking. This could allow an attacker to execute arbitrary code when a legitimate user installs an application that uses the affected setup component.	2025-08-12	8.5
CVE-2025-40759	siemens - multiple products	A vulnerability has been identified in SIMATIC S7-PLCSIM V17 (All versions), SIMATIC STEP 7 V17 (All versions), SIMATIC STEP 7 V18 (All versions), SIMATIC STEP 7 V19 (All versions < V19 Update 4), SIMATIC STEP 7 V20 (All versions), SIMATIC WinCC V17 (All versions), SIMATIC WinCC V18 (All versions), SIMATIC WinCC V19 (All versions < V19 Update 4), SIMATIC WinCC V20 (All versions), SIMOCODE ES V17 (All versions), SIMOCODE ES V18 (All versions), SIMOCODE ES V19 (All versions), SIMOCODE ES V20 (All versions), SIMOTION SCOUT TIA V5.4 (All versions), SIMOTION SCOUT TIA V5.5 (All versions), SIMOTION SCOUT TIA V5.6 (All versions < V5.6 SP1 HF7), SIMOTION SCOUT TIA V5.7 (All versions), SINAMICS Startdrive V17 (All versions), SINAMICS Startdrive V18 (All versions), SINAMICS Startdrive V19 (All versions), SINAMICS Startdrive V20 (All versions), SIRIUS Safety ES V17 (TIA Portal) (All versions), SIRIUS Safety ES V18 (TIA Portal) (All versions), SIRIUS Safety ES V19 (TIA Portal) (All versions), SIRIUS Safety ES V20 (TIA Portal) (All versions), SIRIUS Soft Starter ES V17 (TIA Portal) (All versions), SIRIUS Soft Starter ES V18 (TIA Portal) (All versions), SIRIUS Soft Starter ES V19 (TIA Portal) (All versions), SIRIUS Soft Starter ES V20 (TIA Portal) (All versions), TIA Portal Cloud V17 (All versions), TIA Portal Cloud V18 (All versions), TIA Portal Cloud V19 (All versions < V5.2.1.1), TIA Portal Cloud V20 (All versions). Affected products do not properly sanitize stored security properties when parsing project files. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.	2025-08-12	8.5
CVE-2025-20148	cisco - Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to inject arbitrary HTML content into a device-generated document._x000D_ _x000D_ This vulnerability is due to improper validation of user-supplied data. An attacker could exploit this vulnerability by submitting malicious content to an affected device and using the device to generate a document that contains sensitive information. A successful exploit could allow the attacker to alter the standard layout of the device-generated documents, read arbitrary files from the underlying operating system, and conduct server-side request forgery (SSRF) attacks. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of Security Analyst (Read Only).	2025-08-14	8.5
CVE-2025-20251	cisco - multiple products	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, remote attacker to create or delete arbitrary files on the underlying operating system. If critical system files are manipulated, new Remote Access SSL VPN sessions could be denied and existing sessions could be dropped, causing a denial of service (DoS) condition. An exploited device requires a manual reboot to recover._x000D_ _x000D_ This vulnerability is due to insufficient input validation when processing 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 create or delete files on the underlying operating system, which could cause the Remote Access SSL VPN service to become unresponsive._x000D_ To exploit this vulnerability, the attacker must be authenticated as a VPN user of the affected device.	2025-08-14	8.5
CVE-2025-53731	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-08-12	8.4
CVE-2025-53733	microsoft - multiple products	Incorrect conversion between numeric types in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-08-12	8.4

CVE-2025-53740	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-08-12	8.4
CVE-2025-53784	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-08-12	8.4
CVE-2025-49555	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could result in privilege escalation. A high-privileged attacker could trick a victim into executing unintended actions on a web application where the victim is authenticated, potentially allowing unauthorized access or modification of sensitive data. Exploitation of this issue requires user interaction in that a victim must visit a malicious website or click on a crafted link. Scope is changed.	2025-08-12	8.1
CVE-2025-50177	microsoft - multiple products	Use after free in Windows Message Queuing allows an unauthorized attacker to execute code over a network.	2025-08-12	8.1
CVE-2024-26009	fortinet - multiple products	An authentication bypass using an alternate path or channel [CWE-288] vulnerability in Fortinet FortiOS version 6.4.0 through 6.4.15 and before 6.2.16, FortiProxy version 7.4.0 through 7.4.2, 7.2.0 through 7.2.8 and before 7.0.15 & FortiPAM before version 1.2.0 allows an unauthenticated attacker to seize control of a managed device via crafted FGFM requests, if the device is managed by a FortiManager, and if the attacker knows that FortiManager's serial number.	2025-08-12	8.1
CVE-2025-52970	fortinet - multiple products	A improper handling of parameters in Fortinet FortiWeb versions 7.6.3 and below, versions 7.4.7 and below, versions 7.2.10 and below, and 7.0.10 and below may allow an unauthenticated remote attacker with non-public information pertaining to the device and targeted user to gain admin privileges on the device via a specially crafted request.	2025-08-12	8.1
CVE-2025-50160	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	2025-08-12	8
CVE-2025-50162	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	2025-08-12	8
CVE-2025-50164	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	2025-08-12	8
CVE-2025-53132	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to elevate privileges over a network.	2025-08-12	8
CVE-2025-53720	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to execute code over a network.	2025-08-12	8
CVE-2025-49707	microsoft - ecesv6-series_azure_vm_firmware	Improper access control in Azure Virtual Machines allows an authorized attacker to perform spoofing locally.	2025-08-12	7.9
CVE-2025-49563	adobe - multiple products	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49564	adobe - multiple products	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49761	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-50153	microsoft - multiple products	Use after free in Desktop Windows Manager allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-50155	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-50168	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-50170	microsoft - multiple products	Improper handling of insufficient permissions or privileges in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-50173	microsoft - multiple products	Weak authentication in Windows Installer allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-50176	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Graphics Kernel allows an authorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53133	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53141	microsoft - multiple products	Null pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53149	microsoft - multiple products	Heap-based buffer overflow in Kernel Streaming WOW Thunk Service Driver allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53151	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53152	microsoft - multiple products	Use after free in Desktop Windows Manager allows an authorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53154	microsoft - multiple products	Null pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53155	microsoft - multiple products	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53723	microsoft - multiple products	Numeric truncation error in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53724	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53725	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53726	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-53729	microsoft - multiple products	Improper access control in Azure File Sync allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8

CVE-2025-53730	microsoft - multiple products	Use after free in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53732	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53734	microsoft - multiple products	Use after free in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53735	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53737	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53738	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53739	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53741	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53759	microsoft - multiple products	Use of uninitialized resource in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53761	microsoft - multiple products	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53773	microsoft - visual_studio_2022	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio allows an unauthorized attacker to execute code locally.	2025-08-12	7.8
CVE-2025-53789	microsoft - multiple products	Missing authentication for critical function in Windows StateRepository API allows an authorized attacker to elevate privileges locally.	2025-08-12	7.8
CVE-2025-49560	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49569	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49561	adobe - multiple products	Animate versions 23.0.12, 24.0.9 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49570	adobe - multiple products	Photoshop Desktop versions 25.12.3, 26.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49571	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. If the application uses an uncontrolled search path to locate critical resources such as programs, an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue does not require user interaction.	2025-08-12	7.8
CVE-2025-49572	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-49573	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54187	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54206	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54207	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54208	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54209	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54210	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54211	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54212	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54213	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54215	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8

CVE-2025-54216	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54217	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54218	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54219	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54220	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54221	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54223	adobe - multiple products	InCopy versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54224	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54225	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54226	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54222	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54229	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54230	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54231	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-54232	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	7.8
CVE-2025-8941	red hat - multiple products	A flaw was found in linux-pam. The pam_namespace module may improperly handle user-controlled paths, allowing local users to exploit symlink attacks and race conditions to elevate their privileges to root. This CVE provides a "complete" fix for CVE-2025-6020.	2025-08-13	7.8
CVE-2025-53781	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Azure Virtual Machines allows an authorized attacker to disclose information over a network.	2025-08-12	7.7
CVE-2025-20127	cisco - multiple products	A vulnerability in the TLS 1.3 implementation for a specific cipher for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software for Cisco Firepower 3100 and 4200 Series devices could allow an authenticated, remote attacker to consume resources that are associated with incoming TLS 1.3 connections, which eventually could cause the device to stop accepting any new SSL/TLS or VPN requests._x000D_ _x000D_ This vulnerability is due to the implementation of the TLS 1.3 Cipher TLS_CHACHA20_POLY1305_SHA256. An attacker could exploit this vulnerability by sending a large number of TLS 1.3 connections with the specific TLS 1.3 Cipher TLS_CHACHA20_POLY1305_SHA256. A successful exploit could allow the attacker to cause a denial of service (DoS) condition where no new incoming encrypted connections are accepted. The device must be reloaded to clear this condition._x000D_ Note: These incoming TLS 1.3 connections include both data traffic and user-management traffic. After the device is in the vulnerable state, no new encrypted connections can be accepted.	2025-08-14	7.7
CVE-2025-20244	cisco - multiple products	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow a remote attacker that is authenticated as a VPN user to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to incomplete error checking when parsing an HTTP header field value. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted Remote Access SSL VPN service on an affected device. A successful exploit could allow the attacker to cause a DoS condition, which would cause the affected device to reload.	2025-08-14	7.7
CVE-2024-41979	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 < V2506). The affected application does not enforce mandatory authorization on some functionality level at server side. This could allow an authenticated attacker to gain complete access of the application.	2025-08-12	7.5

CVE-2025-40769	siemens - SINEC Traffic Analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application uses a Content Security Policy that allows unsafe script execution methods. This could allow an attacker to execute unauthorized scripts, potentially leading to cross-site scripting attacks.	2025-08-12	7.5
CVE-2025-40770	siemens - sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions). The affected application uses a monitoring interface that is not operating in a strictly passive mode. This could allow an attacker to interact with the interface, leading to man-in-the-middle attacks.	2025-08-12	7.5
CVE-2025-5456	ivanti - multiple products	A buffer over-read vulnerability in Ivanti Connect Secure before 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to trigger a denial of service. CWE-125	2025-08-12	7.5
CVE-2025-5462	ivanti - multiple products	A heap-based buffer overflow in Ivanti Connect Secure before 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to trigger a denial of service.	2025-08-12	7.5
CVE-2025-33051	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Microsoft Exchange Server allows an unauthorized attacker to disclose information over a network.	2025-08-12	7.5
CVE-2025-49554	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by an Improper Input Validation vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability by providing specially crafted input, causing the application to crash or become unresponsive. Exploitation of this issue does not require user interaction.	2025-08-12	7.5
CVE-2025-49556	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction, and scope is unchanged.	2025-08-12	7.5
CVE-2025-50154	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	7.5
CVE-2025-50169	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB allows an unauthorized attacker to execute code over a network.	2025-08-12	7.5
CVE-2025-53722	microsoft - multiple products	Uncontrolled resource consumption in Windows Remote Desktop Services allows an unauthorized attacker to deny service over a network.	2025-08-12	7.5
CVE-2025-53783	microsoft - multiple products	Heap-based buffer overflow in Microsoft Teams allows an unauthorized attacker to execute code over a network.	2025-08-12	7.5
CVE-2025-53793	microsoft - multiple products	Improper authentication in Azure Stack allows an unauthorized attacker to disclose information over a network.	2025-08-12	7.5
CVE-2025-48989	apache - multiple products	Improper Resource Shutdown or Release vulnerability in Apache Tomcat made Tomcat vulnerable to the made you reset attack. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.9, from 10.1.0-M1 through 10.1.43 and from 9.0.0.M1 through 9.0.107. Older, EOL versions may also be affected. Users are recommended to upgrade to one of versions 11.0.10, 10.1.44 or 9.0.108 which fix the issue.	2025-08-13	7.5
CVE-2025-54472	apache - brpc	Unlimited memory allocation in redis protocol parser in Apache bRPC (all versions < 1.14.1) on all platforms allows attackers to crash the service via network. Root Cause: In the bRPC Redis protocol parser code, memory for arrays or strings of corresponding sizes is allocated based on the integers read from the network. If the integer read from the network is too large, it may cause a bad alloc error and lead to the program crashing. Attackers can exploit this feature by sending special data packets to the bRPC service to carry out a denial-of-service attack on it. The bRPC 1.14.0 version tried to fix this issue by limited the memory allocation size, however, the limitation checking code is not well implemented that may cause integer overflow and evade such limitation. So the 1.14.0 version is also vulnerable, although the integer range that affect version 1.14.0 is different from that affect version < 1.14.0. Affected scenarios: Using bRPC as a Redis server to provide network services to untrusted clients, or using bRPC as a Redis client to call untrusted Redis services. How to Fix: we provide two methods, you can choose one of them: 1. Upgrade bRPC to version 1.14.1. 2. Apply this patch (https://github.com/apache/brpc/pull/3050) manually. No matter you choose which method, you should note that the patch limits the maximum length of memory allocated for each time in the bRPC Redis parser. The default limit is 64M. If some of you redis request or response have a size larger than 64M, you might encounter error after upgrade. For such case, you can modify the gflag redis_max_allocation_size to set a larger limit.	2025-08-14	7.5
CVE-2025-40762	siemens - multiple products	A vulnerability has been identified in Simcenter Femap V2406 (All versions < V2406.0003), Simcenter Femap V2412 (All versions < V2412.0002). The affected applications contain an out of	2025-08-12	7.3

		bounds write vulnerability when parsing a specially crafted STP file. This could allow an attacker to execute code in the context of the current process.(ZDI-CAN-26692)		
CVE-2025-40764	siemens - multiple products	A vulnerability has been identified in Simcenter Femap V2406 (All versions < V2406.0003), Simcenter Femap V2412 (All versions < V2412.0002). The affected applications contains an out of bounds read vulnerability while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2025-08-12	7.3
CVE-2025-50159	microsoft - multiple products	Use after free in Remote Access Point-to-Point Protocol (PPP) EAP-TLS allows an authorized attacker to elevate privileges locally.	2025-08-12	7.3
CVE-2025-50161	microsoft - multiple products	Heap-based buffer overflow in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2025-08-12	7.3
CVE-2025-8296	ivanti - avalanche	SQL injection in Ivanti Avalanche before version 6.4.8.8008 allows a remote authenticated attacker with admin privileges to execute arbitrary SQL queries. In certain conditions, this can also lead to remote code execution	2025-08-12	7.2
CVE-2025-8297	ivanti - avalanche	Incomplete restriction of configuration in Ivanti Avalanche before version 6.4.8.8008 allows a remote authenticated attacker with admin privileges to achieve remote code execution	2025-08-12	7.2
CVE-2025-53779	microsoft - windows_server_2025	Relative path traversal in Windows Kerberos allows an authorized attacker to elevate privileges over a network.	2025-08-12	7.2
CVE-2025-49813	fortinet - multiple products	An improper neutralization of special elements used in an OS Command ("OS Command Injection") vulnerability [CWE-78] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a remote and authenticated attacker with low privilege to execute unauthorized code via specifically crafted HTTP parameters.	2025-08-12	7.2
CVE-2025-53744	fortinet - multiple products	An incorrect privilege assignment vulnerability [CWE-266] in FortiOS Security Fabric version 7.6.0 through 7.6.2, 7.4.0 through 7.4.7, 7.2 all versions, 7.0 all versions, 6.4 all versions, may allow a remote authenticated attacker with high privileges to escalate their privileges to super-admin via registering the device to a malicious FortiManager.	2025-08-12	7.2
CVE-2025-53760	microsoft - multiple products	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2025-08-12	7.1
CVE-2025-40768	siemens - sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application exposes an internal service port to be accessible from outside the system. This could allow an unauthorized attacker to access the application.	2025-08-12	7
CVE-2025-49762	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-50158	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows NTFS allows an unauthorized attacker to disclose information locally.	2025-08-12	7
CVE-2025-50167	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53134	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53135	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows DirectX allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53137	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53140	microsoft - multiple products	Use after free in Kernel Transaction Manager allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53142	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53147	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53718	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53721	microsoft - multiple products	Use after free in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-53788	microsoft - windows_subsystem_for_linux	Time-of-check time-of-use (toctou) race condition in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.	2025-08-12	7
CVE-2025-48500	f5 - multiple products	A missing file integrity check vulnerability exists on MacOS F5 VPN browser client installer that may allow a local, authenticated attacker with access to the local file system to replace it with a malicious package installer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-08-13	7
CVE-2025-43736	liferay - multiple products	A Denial Of Service via File Upload (DOS) vulnerability in the Liferay Portal 7.4.3.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.8, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allows a user to upload more than 300kb profile picture into the user profile. This size more than the noted max 300kb size. This extra amount of data can make Liferay slower.	2025-08-12	6.9
CVE-2025-30034	siemens - simatic_rtls_locating_manager	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.3). Affected devices do not properly validate input sent to its listening port on the local loopback interface. This could allow an unauthenticated local attacker to cause a denial of service condition.	2025-08-12	6.9
CVE-2025-43735	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.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the google_gadget.	2025-08-12	6.9
CVE-2025-54500	f5 - multiple products	An HTTP/2 implementation flaw allows a denial-of-service (DoS) that uses malformed HTTP/2 control frames in order to break the max concurrent streams limit (HTTP/2 MadeYouReset Attack). Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-08-13	6.9

CVE-2025-40584	siemens - multiple products	A vulnerability has been identified in SIMOTION SCOUT TIA V5.4 (All versions), SIMOTION SCOUT TIA V5.5 (All versions), SIMOTION SCOUT TIA V5.6 (All versions < V5.6 SP1 HF7), SIMOTION SCOUT TIA V5.7 (All versions < V5.7 SP1 HF1), SIMOTION SCOUT V5.4 (All versions), SIMOTION SCOUT V5.5 (All versions), SIMOTION SCOUT V5.6 (All versions < V5.6 SP1 HF7), SIMOTION SCOUT V5.7 (All versions < V5.7 SP1 HF1), SINAMICS STARTER V5.5 (All versions), SINAMICS STARTER V5.6 (All versions), SINAMICS STARTER V5.7 (All versions). The affected application contains a XML External Entity Injection (XXE) vulnerability while parsing specially crafted XML files. This could allow an attacker to read arbitrary files in the system.	2025-08-12	6.8
CVE-2025-40752	siemens - multiple products	A vulnerability has been identified in POWER METER SICAM Q100 (7KG9501-0AA01-0AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA01-2AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA31-0AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA31-2AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q200 family (All versions >= V2.70 < V2.80). Affected devices store the password for the SMTP account as plain text. This could allow an authenticated local attacker to extract it and use the configured SMTP service for arbitrary purposes.	2025-08-12	6.8
CVE-2025-40753	siemens - multiple products	A vulnerability has been identified in POWER METER SICAM Q100 (7KG9501-0AA01-0AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA01-2AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA31-0AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q100 (7KG9501-0AA31-2AA1) (All versions >= V2.60 < V2.62), POWER METER SICAM Q200 family (All versions >= V2.70 < V2.80). Affected devices export the password for the SMTP account as plain text in the Configuration File. This could allow an authenticated local attacker to extract it and use the configured SMTP service for arbitrary purposes.	2025-08-12	6.8
CVE-2025-40766	siemens - sinec_traffic_analyzer	A vulnerability has been identified in SINEC Traffic Analyzer (6GK8822-1BG01-0BA0) (All versions < V3.0). The affected application runs docker containers without adequate resource and security limitations. This could allow an attacker to perform a denial-of-service (DoS) attack.	2025-08-12	6.8
CVE-2025-49751	microsoft - multiple products	Missing synchronization in Windows Hyper-V allows an authorized attacker to deny service over an adjacent network.	2025-08-12	6.8
CVE-2025-53736	microsoft - multiple products	Buffer over-read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2025-08-12	6.8
CVE-2024-48892	fortinet - multiple products	A relative path traversal vulnerability [CWE-23] in FortiSOAR 7.6.0, 7.5.0 through 7.5.1, 7.4 all versions, 7.3 all versions may allow an authenticated attacker to read arbitrary files via uploading a malicious solution pack.	2025-08-12	6.8
CVE-2025-48807	microsoft - multiple products	Improper restriction of communication channel to intended endpoints in Windows Hyper-V allows an authorized attacker to execute code locally.	2025-08-12	6.7
CVE-2025-49743	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-08-12	6.7
CVE-2025-27759	fortinet - multiple products	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiWeb version 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2.0 through 7.2.10 and before 7.0.10 allows an authenticated privileged attacker to execute unauthorized code or commands via crafted CLI commands	2025-08-12	6.7
CVE-2025-47857	fortinet - multiple products	A improper neutralization of special elements used in an os command ('os command injection') vulnerability [CWE-78] in Fortinet FortiWeb CLI version 7.6.0 through 7.6.3 and before 7.4.8 allows a privileged attacker to execute arbitrary code or command via crafted CLI commands.	2025-08-12	6.7
CVE-2025-36612	dell - supportassist_for_business_pcs	SupportAssist for Business PCs, version(s) 4.5.3 and prior, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2025-08-14	6.7
CVE-2025-38738	dell - supportassist_for_home_pcs	SupportAssist for Home PCs Installer exe version(s) 4.8.2.29006 and prior, contain(s) an Incorrect Privilege Assignment vulnerability in the Installer. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2025-08-14	6.7
CVE-2025-21110	dell - data_lakehouse	Dell Data Lakehouse, versions prior to 1.5.0.0, contains an Execution with Unnecessary Privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service.	2025-08-14	6.7
CVE-2023-45584	fortinet - multiple products	A double free vulnerability [CWE-415] in Fortinet FortiOS version 7.4.0, version 7.2.0 through 7.2.5 and before 7.0.12, FortiProxy version 7.4.0 through 7.4.1, version 7.2.0 through 7.2.7 and before 7.0.13 and FortiPAM version 1.1.0 through 1.1.2 and before 1.0.3 allows a privileged attacker to execute code or commands via crafted HTTP or HTTPs requests.	2025-08-12	6.6
CVE-2025-8978	d-link - DIR-619L	A vulnerability was determined in D-Link DIR-619L 6.02CN02. Affected is the function FirmwareUpgrade of the component boa. The manipulation leads to insufficient verification of data authenticity. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-08-14	6.6
CVE-2025-8310	ivanti - Virtual Application Delivery ControllerCWE-862	Missing authorization in the admin console of Ivanti Virtual Application Delivery Controller before version 22.9 allows a remote authenticated attacker to take over admin accounts by resetting the password	2025-08-12	6.5
CVE-2025-25005	microsoft - multiple products	Improper input validation in Microsoft Exchange Server allows an authorized attacker to perform tampering over a network.	2025-08-12	6.5
CVE-2025-50166	microsoft - multiple products	Integer overflow or wraparound in Windows Distributed Transaction Coordinator allows an authorized attacker to disclose information over a network.	2025-08-12	6.5
CVE-2025-50172	microsoft - multiple products	Allocation of resources without limits or throttling in Windows DirectX allows an authorized attacker to deny service over a network.	2025-08-12	6.5
CVE-2025-53716	microsoft - multiple products	Null pointer dereference in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.	2025-08-12	6.5
CVE-2025-53728	microsoft - dynamics_365	Exposure of sensitive information to an unauthorized actor in Microsoft Dynamics 365 (on-premises) allows an unauthorized attacker to disclose information over a network.	2025-08-12	6.5
CVE-2025-32932	fortinet - multiple products	An Improper neutralization of input during web page generation ('cross-site scripting') vulnerability [CWE-79] in FortiSOAR version 7.6.1 and below, version 7.5.1 and below, 7.4 all versions, 7.3 all	2025-08-12	6.5

		versions, 7.2 all versions, 7.0 all versions, 6.4 all versions WEB UI may allow an authenticated remote attacker to perform an XSS attack via stored malicious service requests		
CVE-2025-8881	google - chrome	Inappropriate implementation in File Picker in Google Chrome prior to 139.0.7258.127 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2025-08-13	6.5
CVE-2025-55668	apache - multiple products	Session Fixation vulnerability in Apache Tomcat via rewrite valve. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.7, from 10.1.0-M1 through 10.1.41, from 9.0.0.M1 through 9.0.105. Older, EOL versions may also be affected. Users are recommended to upgrade to version 11.0.8, 10.1.42 or 9.0.106, which fix the issue.	2025-08-13	6.5
CVE-2025-20301	cisco - Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure FMC Software could allow an authenticated, low-privileged, remote attacker to access troubleshoot files for a different domain._x000D_ _x000D_ This vulnerability is due to missing authorization checks. An attacker could exploit this vulnerability by directly accessing a troubleshoot file for a different domain that is managed on the same Cisco Secure FMC instance. A successful exploit could allow the attacker to retrieve a troubleshoot file for a different domain, which could allow the attacker to access sensitive information contained in the troubleshoot file.	2025-08-14	6.5
CVE-2025-32766	fortinet - multiple products	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiWeb CLI version 7.6.0 through 7.6.3 and before 7.4.8 allows a privileged attacker to execute arbitrary code or commands via crafted CLI commands	2025-08-12	6.4
CVE-2025-53859	f5 - multiple products	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_mail_smtp_module that might allow an unauthenticated attacker to over-read NGINX SMTP authentication process memory; as a result, the server side may leak arbitrary bytes sent in a request to the authentication server. This issue happens during the NGINX SMTP authentication process and requires the attacker to make preparations against the target system to extract the leaked data. The issue affects NGINX only if (1) it is built with the ngx_mail_smtp_module, (2) the smtp_auth directive is configured with method "none," and (3) the authentication server returns the "Auth-Wait" response header. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-08-13	6.3
CVE-2025-43201	apple - music_classical	This issue was addressed with improved checks. This issue is fixed in Apple Music Classical 2.3 for Android. An app may be able to unexpectedly leak a user's credentials.	2025-08-15	6.2
CVE-2024-41986	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 < V2506). The affected application support insecure TLS 1.0 and 1.1 protocol. An attacker could achieve a man-in-the-middle attack and compromise confidentiality and integrity of data.	2025-08-12	6.1
CVE-2025-20235	cisco - Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	2025-08-14	6.1
CVE-2025-20220	cisco - multiple products	A vulnerability in the CLI of Cisco Secure Firewall Management Center (FMC) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system as root._x000D_ _x000D_ This vulnerability is due to improper input validation for specific CLI commands. An attacker could exploit this vulnerability by injecting operating system commands into a legitimate command. A successful exploit could allow the attacker to escape the restricted command prompt and execute arbitrary commands on the underlying operating system. To successfully exploit this vulnerability, an attacker would need valid Administrator credentials._x000D_ _x000D_ For more information about vulnerable scenarios, see the Details ["#details"] section of this advisory.	2025-08-14	6
CVE-2025-20237	cisco - multiple products	A vulnerability in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. To exploit this vulnerability, the attacker must have valid administrative credentials._x000D_ _x000D_ This vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input for specific commands. A successful exploit could allow the attacker to execute commands on the underlying operating system as root.	2025-08-14	6
CVE-2025-20238	cisco - multiple products	A vulnerability in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system with root-level privileges. To exploit this vulnerability, the attacker must have valid administrative credentials._x000D_ _x000D_ This vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input for specific commands. A successful exploit could allow the attacker to execute commands on the underlying operating system as root.	2025-08-14	6
CVE-2024-41982	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 <	2025-08-12	5.9

		V2506). The affected application does not have adequate encryption of sensitive information. This could allow an authenticated attacker to gain access of sensitive information.		
CVE-2025-49558	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in a security feature bypass. An attacker could exploit this vulnerability by manipulating the timing between the check of a resource's state and its use, allowing unauthorized write access. Exploitation of this issue does not require user interaction.	2025-08-12	5.9
CVE-2025-36124	ibm - websphere_application_server	IBM WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.8 could allow a remote attacker to bypass security restrictions caused by a failure to honor JMS messaging configuration	2025-08-12	5.9
CVE-2025-20224	cisco - multiple products	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to partially exhaust system memory, causing system instability like being unable to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.	2025-08-14	5.8
CVE-2025-20225	cisco - multiple products	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco IOS Software, IOS XE Software, Secure Firewall Adaptive Security Appliance (ASA) Software, and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to a lack of proper processing of IKEv2 packets. An attacker could exploit this vulnerability by sending crafted IKEv2 packets to an affected device. In the case of Cisco IOS and IOS XE Software, a successful exploit could allow the attacker to cause the device to reload unexpectedly. In the case of Cisco ASA and FTD Software, a successful exploit could allow the attacker to partially exhaust system memory, causing system instability such as being unable to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.	2025-08-14	5.8
CVE-2025-20252	cisco - multiple products	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to partially exhaust system memory, causing system instability like being unable to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.	2025-08-14	5.8
CVE-2025-20254	cisco - multiple products	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) module of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a memory leak, resulting in a denial of service (DoS) condition._x000D_ _x000D_ This vulnerability is due to improper parsing of IKEv2 packets. An attacker could exploit this vulnerability by sending a continuous stream of crafted IKEv2 packets to an affected device. A successful exploit could allow the attacker to partially exhaust system memory, causing system instability like being unable to establish new IKEv2 VPN sessions. A manual reboot of the device is required to recover from this condition.	2025-08-14	5.8
CVE-2025-20268	cisco - Cisco Firepower Threat Defense Software	A vulnerability in the Geolocation-Based Remote Access (RA) VPN feature of Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured policies to allow or deny HTTP connections based on a country or region._x000D_ _x000D_ This vulnerability exists because the URL string is not fully parsed. An attacker could exploit this vulnerability by sending a crafted HTTP connection through the targeted device. A successful exploit could allow the attacker to bypass configured policies and gain access to a network where the connection should have been denied.	2025-08-14	5.8
CVE-2025-50156	microsoft - multiple products	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.	2025-08-12	5.7
CVE-2025-50157	microsoft - multiple products	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.	2025-08-12	5.7
CVE-2025-53138	microsoft - multiple products	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.	2025-08-12	5.7
CVE-2025-53148	microsoft - multiple products	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.	2025-08-12	5.7
CVE-2025-53153	microsoft - multiple products	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.	2025-08-12	5.7
CVE-2025-53719	microsoft - multiple products	Use of uninitialized resource in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to disclose information over a network.	2025-08-12	5.7
CVE-2025-26398	solarwinds - Database Performance Analyzer	SolarWinds Database Performance Analyzer was found to contain a hard-coded cryptographic key. If exploited, this vulnerability could lead to a machine-in-the-middle (MITM) attack against users. This vulnerability requires additional software not installed by default, local access to the server and administrator level privileges on the host.	2025-08-12	5.6
CVE-2025-5468	ivanti - multiple products	Improper handling of symbolic links in Ivanti Connect Secure before version 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a local authenticated attacker to read arbitrary files on disk.	2025-08-12	5.5
CVE-2025-49567	adobe - multiple products	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this	2025-08-12	5.5

		vulnerability to crash the application, causing a disruption in service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.		
CVE-2025-49568	adobe - multiple products	Illustrator versions 28.7.8, 29.6.1 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-53136	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows NT OS Kernel allows an authorized attacker to disclose information locally.	2025-08-12	5.5
CVE-2025-53156	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Storage Port Driver allows an authorized attacker to disclose information locally.	2025-08-12	5.5
CVE-2025-53769	microsoft - windows_security_app	External control of file name or path in Windows Security App allows an authorized attacker to perform spoofing locally.	2025-08-12	5.5
CVE-2024-52964	fortinet - multiple products	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiManager version 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.9 and below 7.0.13 & FortiManager Cloud version 7.6.0 through 7.6.1, 7.4.0 through 7.4.5 and before 7.2.9 allows an authenticated remote attacker to overwrite arbitrary files via FGFM crafted requests.	2025-08-12	5.5
CVE-2025-49562	adobe - multiple products	Animate versions 23.0.12, 24.0.9 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54186	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54188	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54189	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54190	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54191	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54192	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54193	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54194	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54195	adobe - substance_3d_painter	Substance3D - Painter versions 11.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54197	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54198	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54199	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54200	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54201	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54202	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54203	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54204	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54205	adobe - substance_3d_sampler	Substance3D - Sampler versions 5.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54214	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5

CVE-2025-54227	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54228	adobe - multiple products	InDesign Desktop versions 20.4, 19.5.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54235	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.0 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54233	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-54238	adobe - dimension	Dimension versions 4.1.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-08-12	5.5
CVE-2025-26484	dell - cloudlink	Dell CloudLink, versions 8.0 through 8.1.1, contains an Improper Restriction of XML External Entity Reference vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	2025-08-14	5.5
CVE-2025-49745	microsoft - dynamics_365	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Dynamics 365 (on-premises) allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	5.4
CVE-2025-36088	ibm - Storage TS4500 Library	IBM TS4500 1.11.0.0-D00, 1.11.0.1-C00, 1.11.0.2-C00, and 1.10.00-F00 web GUI 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.	2025-08-15	5.4
CVE-2025-25006	microsoft - multiple products	Improper handling of additional special element in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	5.3
CVE-2025-25007	microsoft - multiple products	Improper validation of syntactic correctness of input in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	5.3
CVE-2025-49559	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha1, 2.4.8-p1, 2.4.7-p6, 2.4.6-p11, 2.4.5-p13, 2.4.4-p14 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to modify limited data. Exploitation of this issue does not require user interaction.	2025-08-12	5.3
CVE-2025-25248	fortinet - multiple products	An Integer Overflow or Wraparound vulnerability [CWE-190] in FortiOS version 7.6.2 and below, version 7.4.7 and below, version 7.2.10 and below, 7.2 all versions, 6.4 all versions, FortiProxy version 7.6.2 and below, version 7.4.3 and below, 7.2 all versions, 7.0 all versions, 2.0 all versions and FortiPAM version 1.5.0, version 1.4.2 and below, 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions SSL-VPN RDP and VNC bookmarks may allow an authenticated user to affect the device SSL-VPN availability via crafted requests.	2025-08-12	5.3
CVE-2025-55672	apache - superset	A stored Cross-Site Scripting (XSS) vulnerability exists in Apache Superset's chart visualization. An authenticated user with permissions to edit charts can inject a malicious payload into a column's label. The payload is not properly sanitized and gets executed in the victim's browser when they hover over the chart, potentially leading to session hijacking or the execution of arbitrary commands on behalf of the user. This issue affects Apache Superset: before 5.0.0. Users are recommended to upgrade to version 5.0.0, which fixes the issue.	2025-08-14	5.3
CVE-2025-55673	apache - superset	When a guest user accesses a chart in Apache Superset, the API response from the /chart/data endpoint includes a query field in its payload. This field contains the underlying query, which improperly discloses database schema information, such as table names, to the low-privileged guest user. This issue affects Apache Superset: before 4.1.3. Users are recommended to upgrade to version 4.1.3, which fixes the issue.	2025-08-14	5.3
CVE-2025-55674	apache - superset	A bypass of the DISALLOWED_SQL_FUNCTIONS security feature in Apache Superset allows for the execution of blocked SQL functions. An attacker can use a special inline block to circumvent the denylist. This allows a user with SQL Lab access to execute functions that were intended to be disabled, leading to the disclosure of sensitive database information like the software version. This issue affects Apache Superset: before 5.0.0. Users are recommended to upgrade to version 5.0.0, which fixes the issue.	2025-08-14	5.3
CVE-2025-55675	apache - superset	Apache Superset contains an improper access control vulnerability in its /explore endpoint. A missing authorization check allows an authenticated user to discover metadata about datasources they do not have permission to access. By iterating through the datasource_id in the URL, an attacker can enumerate and confirm the existence and names of protected datasources, leading to sensitive information disclosure. This issue affects Apache Superset: before 5.0.0. Users are recommended to upgrade to version 5.0.0, which fixes the issue.	2025-08-14	5.3
CVE-2025-33142	ibm - multiple products	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security for TLS connections.	2025-08-14	5.3
CVE-2025-36047	ibm - websphere_application_server	IBM WebSphere Application Server Liberty 18.0.0.2 through 25.0.0.8 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	2025-08-14	5.3
CVE-2025-20219	cisco - multiple products	A vulnerability in the implementation of access control rules for loopback interfaces in Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD)	2025-08-14	5.3

		Software could allow an unauthenticated, remote attacker to send traffic that should have been blocked to a loopback interface._x000D_ _x000D_ This vulnerability is due to improper enforcement of access control rules for loopback interfaces. An attacker could exploit this vulnerability by sending traffic to a loopback interface on an affected device. A successful exploit could allow the attacker to bypass configured access control rules and send traffic that should have been blocked to a loopback interface on the device.		
CVE-2024-41983	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 < V2506). The affected application displays SQL statement in the error messages encountered during the generation of reports using Cockpit tool.	2025-08-12	5.1
CVE-2025-33023	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions), RUGGEDCOM ROX MX5000RE (All versions), RUGGEDCOM ROX RX1400 (All versions), RUGGEDCOM ROX RX1500 (All versions), RUGGEDCOM ROX RX1501 (All versions), RUGGEDCOM ROX RX1510 (All versions), RUGGEDCOM ROX RX1511 (All versions), RUGGEDCOM ROX RX1512 (All versions), RUGGEDCOM ROX RX1524 (All versions), RUGGEDCOM ROX RX1536 (All versions), RUGGEDCOM ROX RX5000 (All versions). The affected devices do not properly enforce the restriction of files that can be uploaded from the web interface. This could allow an authenticated remote attacker with high privileges in the web interface to upload arbitrary files.	2025-08-12	5.1
CVE-2025-43734	liferay - multiple products	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.10, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.1 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.16 and 7.4 GA through update 92 allows a remote authenticated attacker to inject JavaScript code in the “first display label” field in the configuration of a custom sort widget. This malicious payload is then reflected and executed by clay button taglib when refreshing the page.	2025-08-12	5.1
CVE-2025-9003	d-link - DIR-818LW	A vulnerability has been found in D-Link DIR-818LW 1.04. This vulnerability affects unknown code of the file /bsc_lan.php of the component DHCP Reserved Address Handler. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-08-15	5.1
CVE-2025-5466	ivanti - multiple products	XEE in Ivanti Connect Secure before 22.7R2.8 or 22.8R2, Ivanti Policy Secure before 22.7R1.5, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to trigger a denial of service	2025-08-12	4.9
CVE-2025-20218	cisco - Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to retrieve sensitive information from an affected device._x000D_ _x000D_ This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to retrieve sensitive information from the affected device._x000D_ To exploit this vulnerability, the attacker must have valid administrative credentials.	2025-08-14	4.9
CVE-2025-20306	cisco - Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker with Administrator-level privileges to execute arbitrary commands on the underlying operating system._x000D_ _x000D_ This vulnerability is due to insufficient input validation of certain HTTP request parameters that are sent to the web-based management interface. An attacker could exploit this vulnerability by authenticating to the interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute commands as the root user on the affected device. To exploit this vulnerability, an attacker would need Administrator-level credentials.	2025-08-14	4.9
CVE-2025-40751	siemens - simatic_rtls_locating_manager	A vulnerability has been identified in SIMATIC RTLS Locating Manager (All versions < V3.3). Affected SIMATIC RTLS Locating Manager Report Clients do not properly protect credentials that are used to authenticate to the server. This could allow an authenticated local attacker to extract the credentials and use them to escalate their access rights from the Manager to the Systemadministrator role.	2025-08-12	4.8
CVE-2025-38745	dell - multiple products	Dell OpenManage Enterprise, versions 3.10, 4.0, 4.1, and 4.2, contains an Insertion of Sensitive Information into Log File vulnerability in the Backup and Restore. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2025-08-14	4.8
CVE-2025-53765	microsoft - azure_app_service_on_azure_stack	Exposure of private personal information to an unauthorized actor in Azure Stack allows an authorized attacker to disclose information locally.	2025-08-12	4.4
CVE-2024-40588	fortinet - forticamera_firmware	Multiple relative path traversal vulnerabilities [CWE-23] in Fortinet FortiMail version 7.6.0 through 7.6.1 and before 7.4.3, FortiVoice version 7.0.0 through 7.0.5 and before 7.4.9, FortiRecorder version 7.2.0 through 7.2.1 and before 7.0.4, FortiCamera & FortiNDR version 7.6.0 and before 7.4.6 may allow a privileged attacker to read files from the underlying filesystem via crafted CLI requests.	2025-08-12	4.4
CVE-2025-36000	ibm - websphere_application_server	IBM WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.8 is vulnerable to stored 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.	2025-08-12	4.4
CVE-2025-49736	microsoft - edge	The ui performs the wrong action in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	4.3
CVE-2025-49755	microsoft - edge	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	2025-08-12	4.3
CVE-2025-20135	cisco - multiple products	A vulnerability in the DHCP client functionality of Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an	2025-08-14	4.3

		unauthenticated, adjacent attacker to exhaust available memory._x000D_ _x000D_ This vulnerability is due to improper validation of incoming DHCP packets. An attacker could exploit this vulnerability by repeatedly sending crafted DHCPv4 packets to an affected device. A successful exploit could allow the attacker to exhaust available memory, which would affect availability of services and prevent new processes from starting, resulting in a Denial of Service (DoS) condition that would require a manual reboot._x000D_ Note: On Cisco Secure FTD Software, this vulnerability does not affect management interfaces.		
CVE-2025-20302	cisco - Cisco Firepower Management Center	A vulnerability in the web-based management interface of Cisco Secure FMC Software could allow an authenticated, low-privileged, remote attacker to retrieve a generated report from a different domain._x000D_ _x000D_ This vulnerability is due to missing authorization checks. An attacker could exploit this vulnerability by directly accessing a generated report file for a different domain that is managed on the same Cisco Secure FMC instance. A successful exploit could allow the attacker to access a previously run report for a different domain, which could allow an attacker to read activity recorded in that domain.	2025-08-14	4.3
CVE-2025-36581	dell - PowerEdge	Dell PowerEdge Platform version(s) 14G AMD BIOS v1.25.0 and prior, contain(s) an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2025-08-14	3.8
CVE-2025-36613	dell - multiple products	SupportAssist for Home PCs versions 4.6.3 and prior and SupportAssist for Business PCs versions 4.5.3 and prior, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.	2025-08-14	2.8
CVE-2025-40570	siemens - multiple products	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V10.0), SIPROTEC 5 6MD85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 6MD86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 6MD89 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 6MU85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7KE85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SA82 (CP150) (All versions < V10.0), SIPROTEC 5 7SA86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SA87 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SD82 (CP150) (All versions < V10.0), SIPROTEC 5 7SD86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SD87 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SJ81 (CP150) (All versions < V10.0), SIPROTEC 5 7SJ82 (CP150) (All versions < V10.0), SIPROTEC 5 7SJ85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SJ86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SK82 (CP150) (All versions < V10.0), SIPROTEC 5 7SK85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SL82 (CP150) (All versions < V10.0), SIPROTEC 5 7SL86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SL87 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7SS85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7ST85 (CP300) (All versions < V10.0), SIPROTEC 5 7ST86 (CP300) (All versions < V10.0), SIPROTEC 5 7SX82 (CP150) (All versions < V10.0), SIPROTEC 5 7SX85 (CP300) (All versions < V10.0), SIPROTEC 5 7SY82 (CP150) (All versions < V10.0), SIPROTEC 5 7UM85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7UT82 (CP150) (All versions < V10.0), SIPROTEC 5 7UT85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7UT86 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7UT87 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7VE85 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7VK87 (CP300) (All versions >= V7.80 < V10.0), SIPROTEC 5 7VU85 (CP300) (All versions < V10.0), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V10.0). Affected devices do not properly limit the bandwidth for incoming network packets over their local USB port. This could allow an attacker with physical access to send specially crafted packets with high bandwidth to the affected devices thus forcing them to exhaust their memory and stop responding to any network traffic via the local USB port. Affected devices reset themselves automatically after a successful attack. The protection function is not affected of this vulnerability.	2025-08-12	2.4
CVE-2024-41984	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 < V2506). The affected application improperly handles error while accessing an inaccessible resource leading to exposing the system applications.	2025-08-12	2.1
CVE-2024-41985	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 < V2506). The affected application does not expire the session without logout. This could allow an attacker to get unauthorized access if the session is left idle.	2025-08-12	2.1
CVE-2024-41980	siemens - multiple products	A vulnerability has been identified in SmartClient modules Opcenter QL Home (SC) (All versions >= V13.2 < V2506), SOA Audit (All versions >= V13.2 < V2506), SOA Cockpit (All versions >= V13.2 < V2506). The affected application do not encrypt the communication in LDAP interface by default. This could allow an authenticated attacker to gain unauthorized access to sensitive information.	2025-08-12	2