الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 6th of July to 12th of July. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٦ يوليو إلى ١٢ يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-47981	microsoft - multiple products	Heap-based buffer overflow in Windows SPNEGO Extended Negotiation allows an unauthorized attacker to execute code over a network.	2025-07-08	9.8
CVE-2025-37103	hewlett packard enterprise (hpe) - HPE Networking Instant On	Hard-coded login credentials were found in HPE Networking Instant On Access Points, allowing anyone with knowledge of it to bypass normal device authentication. Successful exploitation could allow a remote attacker to gain administrative access to the system.	2025-07-08	9.8
CVE-2025-49533	adobe - experience_manager	Adobe Experience Manager (MS) versions 6.5.23.0 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could lead to arbitrary code execution by an attacker. Exploitation of this issue does not require user interaction. Scope is unchanged.	2025-07-08	9.8
CVE-2023-38036	ivanti - avalanche	A security vulnerability within Ivanti Avalanche Manager before version 6.4.1 may allow an unauthenticated attacker to create a buffer overflow that could result in service disruption or arbitrary code execution.	2025-07-12	9.8
CVE-2025-27203	adobe - connect	Adobe Connect versions 24.0 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could lead to arbitrary code execution by an attacker. Exploitation of this issue does require user interaction and scope is changed.	2025-07-08	9.6
CVE-2025-40736	siemens - SINEC NMS	A vulnerability has been identified in SINEC NMS (All versions < V4.0). The affected application exposes an endpoint that allows an unauthorized modification of administrative credentials. This could allow an unauthenticated attacker to reset the superadmin password and gain full control of the application (ZDI-CAN-26569).	2025-07-08	9.3
CVE-2025-49535	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in a Security feature bypass. An attacker could exploit this vulnerability to access sensitive information or denial of service by bypassing security measures. Exploitation of this issue does not require user interaction and scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	9.3
CVE-2025-21450	qualcomm - ar8035_firmware	Cryptographic issue occurs due to use of insecure connection method while downloading.	2025-07-08	9.1
CVE-2025-23048	apache software foundation - Apache HTTP Server	In some mod_ssl configurations on Apache HTTP Server 2.4.35 through to 2.4.63, an access control bypass by trusted clients is possible using TLS 1.3 session resumption. Configurations are affected when mod_ssl is configured for multiple virtual hosts, with each restricted to a different set of trusted client certificates (for example with a different SSLCACertificateFile/Path setting). In such a case, a client trusted to access one virtual host may be able to access another virtual host, if SSLStrictSNIVHostCheck is not enabled in either virtual host.	2025-07-10	9.1
CVE-2025-47986	microsoft - multiple products	Use after free in Universal Print Management Service allows an authorized attacker to elevate privileges locally.	2025-07-08	8.8
CVE-2025-47998	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.	2025-07-08	8.8
CVE-2025-48817	microsoft - multiple products	Relative path traversal in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2025-07-08	8.8
CVE-2025-48824	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.	2025-07-08	8.8

CVE-2025-49657	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.	2025-07-08	8.8
CVE-2025-49663	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.	2025-07-08	8.8
CVE-2025-49668	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.	2025-07-08	8.8
CVE-2025-49669	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.	2025-07-08	8.8
CVE-2025-49672	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.	2025-07-08	8.8
CVE-2025-49673	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.	2025-07-08	8.8
CVE-2025-49674	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.	2025-07-08	8.8
CVE-2025-49676	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.	2025-07-08	8.8
CVE-2025-49687	microsoft - multiple products	Out-of-bounds read in Microsoft Input Method Editor (IME) allows an authorized attacker to elevate privileges locally.	2025-07-08	8.8
CVE-2025-49688	microsoft - multiple products	Double free in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	2025-07-08	8.8
CVE-2025-49701	microsoft - multiple products	Improper authorization in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-07-08	8.8
CVE-2025-49704	microsoft - multiple products	Improper control of generation of code ('code injection') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-07-08	8.8
CVE-2025-49723	microsoft - multiple products	Missing authorization in Windows StateRepository API allows an authorized attacker to perform tampering locally.	2025-07-08	8.8
CVE-2025-49724	microsoft - multiple products	Use after free in Windows Connected Devices Platform Service allows an unauthorized attacker to execute code over a network.	2025-07-08	8.8
CVE-2025-49729	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.	2025-07-08	8.8
CVE-2025-49739	microsoft - multiple products	Improper link resolution before file access ('link following') in Visual Studio allows an unauthorized attacker to elevate privileges over a network.	2025-07-08	8.8
CVE-2025-49740	microsoft - multiple products	Protection mechanism failure in Windows SmartScreen allows an unauthorized attacker to bypass a security feature over a network.	2025-07-08	8.8
CVE-2025-49753	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.	2025-07-08	8.8
CVE-2025-49551	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a Use of Hard-coded Credentials vulnerability that could result in privilege escalation. An attacker could leverage this vulnerability to gain unauthorized access to sensitive systems or data. Exploitation of this issue does not require user interaction. The vulnerable component is restricted to internal IP addresses.	2025-07-08	8.8
CVE-2025-40735	siemens - SINEC NMS	A vulnerability has been identified in SINEC NMS (All versions < V4.0). The affected devices are vulnerable to SQL injection. This could allow an unauthenticated remote attacker to execute arbitrary SQL queries on the server database.	2025-07-08	8.7
CVE-2025-40737	siemens - SINEC NMS	A vulnerability has been identified in SINEC NMS (All versions < V4.0). The affected application does not properly validate file paths when extracting uploaded ZIP files. This could allow an attacker to write arbitrary files to restricted locations and potentially execute code with elevated privileges (ZDI-CAN-26571).	2025-07-08	8.7
CVE-2025-40738	siemens - SINEC NMS	A vulnerability has been identified in SINEC NMS (All versions < V4.0). The affected application does not properly validate file paths when extracting uploaded ZIP files. This could allow an attacker to write arbitrary files to restricted locations and potentially execute code with elevated privileges (ZDI-CAN-26572).	2025-07-08	8.7
CVE-2025-48822	microsoft - multiple products	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2025-07-08	8.6
CVE-2025-23365	siemens - TIA Administrator	A vulnerability has been identified in TIA Administrator (All versions < V3.0.6). The affected application allows low-privileged users to trigger installations by overwriting cache files and modifying the downloads path. This would allow an attacker to escalate privilege and exceute arbitrary code.	2025-07-08	8.5
CVE-2025-49717	microsoft - multiple products	Heap-based buffer overflow in SQL Server allows an authorized attacker to execute code over a network.	2025-07-08	8.5
CVE-2025-6995	ivanti - multiple products	Improper use of encryption in the agent of Ivanti Endpoint Manager before version 2024 SU3 and 2022 SU8 Security Update 1 allows a local authenticated attacker to decrypt other users’ passwords.	2025-07-08	8.4
CVE-2025-6996	ivanti - multiple products	Improper use of encryption in the agent of Ivanti Endpoint Manager before version 2024 SU3 and 2022 SU8 Security Update 1 allows a local authenticated attacker to decrypt other users’ passwords.	2025-07-08	8.4
CVE-2025-49695	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-07-08	8.4
CVE-2025-49696	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-07-08	8.4
CVE-2025-49697	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-07-08	8.4
CVE-2025-36014	ibm - Integration Bus	IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.5 is vulnerable to code injection by a privileged user with access to the IIB install directory.	2025-07-07	8.2
CVE-2025-21427	qualcomm - sm6250_firmware	Information disclosure while decoding this RTP packet Payload when UE receives the RTP packet from the network.	2025-07-08	8.2
CVE-2025-36600	dell - Client Platform BIOS	Dell Client Platform BIOS contains an Improper Access Control Applied to Mirrored or Aliased Memory Regions vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2025-07-08	8.2
CVE-2025-53652	jenkins - git_parameter	Jenkins Git Parameter Plugin 439.vb_0e46ca_14534 and earlier does not validate that the Git parameter value submitted to the build matches one of the offered choices, allowing attackers with Item/Build permission to inject arbitrary values into Git parameters.	2025-07-09	8.2

CVE-2025-33054	microsoft - multiple products	Insufficient UI warning of dangerous operations in Remote Desktop Client allows an unauthorized attacker to perform spoofing over a network.	2025-07-08	8.1
CVE-2025-49735	microsoft - multiple products	Use after free in Windows KDC Proxy Service (KPSSVC) allows an unauthorized attacker to execute code over a network.	2025-07-08	8.1
CVE-2025-47178	microsoft - Microsoft Configuration Manager	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Configuration Manager allows an authorized attacker to execute code over an adjacent network.	2025-07-08	8
CVE-2025-47972	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Input Method Editor (IME) allows an authorized attacker to elevate privileges over a network.	2025-07-08	8
CVE-2025-49691	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code over an adjacent network.	2025-07-08	8
CVE-2025-49537	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code execution by a high-privileged attacker. Exploitation of this issue requires user interaction and scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	7.9
CVE-2025-27446	apache - apisix	Incorrect Permission Assignment for Critical Resource vulnerability in Apache APISIX(java-plugin-runner). Local listening file permissions in APISIX plugin runner allow a local attacker to elevate privileges. This issue affects Apache APISIX(java-plugin-runner): from 0.2.0 through 0.5.0. Users are recommended to upgrade to version 0.6.0 or higher, which fixes the issue.	2025-07-06	7.8
CVE-2025-21432	qualcomm - aqt1000_firmware	Memory corruption while retrieving the CBOR data from TA.	2025-07-08	7.8
CVE-2025-21444	qualcomm - qam8255p_firmware	Memory corruption while copying the result to the transmission queue in EMAC.	2025-07-08	7.8
CVE-2025-21445	qualcomm - qam8255p_firmware	Memory corruption while copying the result to the transmission queue which is shared between the virtual machine and the host.	2025-07-08	7.8
CVE-2025-21466	qualcomm - aqt1000_firmware	Memory corruption while processing a private escape command in an event trigger.	2025-07-08	7.8
CVE-2025-27042	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while processing video packets received from video firmware.	2025-07-08	7.8
CVE-2025-27043	qualcomm - ar8035_firmware	Memory corruption while processing manipulated payload in video firmware.	2025-07-08	7.8
CVE-2025-27044	qualcomm - fastconnect_6900_firmware	Memory corruption while executing timestamp video decode command with large input values.	2025-07-08	7.8
CVE-2025-27046	qualcomm - aqt1000_firmware	Memory corruption while processing multiple simultaneous escape calls.	2025-07-08	7.8
CVE-2025-27047	qualcomm - fastconnect_6700_firmware	Memory corruption while processing the TESTPATTERNCONFIG escape path.	2025-07-08	7.8
CVE-2025-27050	qualcomm - aqt1000_firmware	Memory corruption while processing event close when client process terminates abruptly.	2025-07-08	7.8
CVE-2025-27051	qualcomm - fastconnect_6900_firmware	Memory corruption while processing command message in WLAN Host.	2025-07-08	7.8
CVE-2025-27052	qualcomm - ar8035_firmware	Memory corruption while processing data packets in diag received from Unix clients.	2025-07-08	7.8
CVE-2025-27055	qualcomm - aqt1000_firmware	Memory corruption during the image encoding process.	2025-07-08	7.8
CVE-2025-27056	qualcomm - fastconnect_7800_firmware	Memory corruption during sub-system restart while processing clean-up to free up resources.	2025-07-08	7.8
CVE-2025-27058	qualcomm - fastconnect_6900_firmware	Memory corruption while processing packet data with exceedingly large packet.	2025-07-08	7.8
CVE-2025-27061	qualcomm - 315_5g_iot_firmware	Memory corruption whhile handling the subsystem failure memory during the parsing of video packets received from the video firmware.	2025-07-08	7.8
CVE-2025-21164	adobe - substance_3d_designer	Substance3D - Designer versions 14.1 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.	2025-07-08	7.8
CVE-2025-21165	adobe - substance_3d_designer	Substance3D - Designer versions 14.1 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.	2025-07-08	7.8
CVE-2025-21166	adobe - substance_3d_designer	Substance3D - Designer versions 14.1 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.	2025-07-08	7.8
CVE-2025-47159	microsoft - multiple products	Protection mechanism failure in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47971	microsoft - multiple products	Buffer over-read in Virtual Hard Disk (VHDX) allows an unauthorized attacker to elevate privileges locally.	2025-07-08	7.8

CVE-2025-47973	microsoft - multiple products	Buffer over-read in Virtual Hard Disk (VHDX) allows an unauthorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47976	microsoft - multiple products	Use after free in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47982	microsoft - multiple products	Improper input validation in Windows Storage VSP Driver allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47985	microsoft - multiple products	Untrusted pointer dereference in Windows Event Tracing allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47987	microsoft - multiple products	Heap-based buffer overflow in Windows Cred SSProvider Protocol allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47991	microsoft - multiple products	Use after free in Microsoft Input Method Editor (IME) allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47993	microsoft - multiple products	Improper access control in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47994	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office allows an unauthorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-47996	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows MBT Transport driver allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-48000	microsoft - multiple products	Use after free in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-48799	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Update Service allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-48805	microsoft - multiple products	Heap-based buffer overflow in Microsoft MPEG-2 Video Extension allows an authorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-48806	microsoft - multiple products	Use after free in Microsoft MPEG-2 Video Extension allows an authorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-48815	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-48816	microsoft - multiple products	Integer overflow or wraparound in HID class driver allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-48820	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows AppX Deployment Service allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49659	microsoft - multiple products	Buffer over-read in Windows TDX.sys allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49660	microsoft - multiple products	Use after free in Windows Event Tracing allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49661	microsoft - multiple products	Untrusted pointer dereference in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49665	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Workspace Broker allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49667	microsoft - multiple products	Double free in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49675	microsoft - multiple products	Use after free in Kernel Streaming WOW Thunk Service Driver allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49679	microsoft - multiple products	Numeric truncation error in Windows Shell allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49683	microsoft - multiple products	Integer overflow or wraparound in Virtual Hard Disk (VHDX) allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49686	microsoft - multiple products	Null pointer dereference in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49689	microsoft - multiple products	Integer overflow or wraparound in Virtual Hard Disk (VHDX) allows an unauthorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49693	microsoft - multiple products	Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49694	microsoft - multiple products	Null pointer dereference in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49698	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49700	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49702	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49703	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49705	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49711	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49714	microsoft - python	Trust boundary violation in Visual Studio Code - Python extension allows an unauthorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-49721	microsoft - multiple products	Heap-based buffer overflow in Windows Fast FAT Driver allows an unauthorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49725	microsoft - multiple products	Use after free in Windows Notification allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49726	microsoft - multiple products	Use after free in Windows Notification allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49730	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Microsoft Windows QoS scheduler allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8

CVE-2025-49732	microsoft - multiple products	Heap-based buffer overflow in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49733	microsoft - multiple products	Use after free in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49738	microsoft - Microsoft PC Manager	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2025-07-08	7.8
CVE-2025-49742	microsoft - multiple products	Integer overflow or wraparound in Microsoft Graphics Component allows an authorized attacker to execute code locally.	2025-07-08	7.8
CVE-2025-30312	adobe - dimension	Dimension versions 4.1.2 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.	2025-07-08	7.8
CVE-2025-43582	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.22 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, scope unchanged. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	7.8
CVE-2025-43591	adobe - multiple products	InDesign Desktop versions 19.5.3 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.	2025-07-08	7.8
CVE-2025-43592	adobe - multiple products	InDesign Desktop versions 19.5.3 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.	2025-07-08	7.8
CVE-2025-43594	adobe - multiple products	InDesign Desktop versions 19.5.3 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.	2025-07-08	7.8
CVE-2025-47103	adobe - multiple products	InDesign Desktop versions 19.5.3 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.	2025-07-08	7.8
CVE-2025-47134	adobe - multiple products	InDesign Desktop versions 19.5.3 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.	2025-07-08	7.8
CVE-2025-47136	adobe - multiple products	InDesign Desktop versions 19.5.3 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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.	2025-07-08	7.8
CVE-2025-49526	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	7.8
CVE-2025-49527	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	7.8
CVE-2025-49528	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	7.8
CVE-2025-49529	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	7.8
CVE-2025-49530	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	7.8
CVE-2025-49531	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 and earlier are affected by an Integer Overflow or Wraparound 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.	2025-07-08	7.8
CVE-2025-49532	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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.	2025-07-08	7.8
CVE-2025-47097	adobe - multiple products	InCopy versions 20.3, 19.5.3 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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.	2025-07-08	7.8
CVE-2025-47098	adobe - multiple products	InCopy versions 20.3, 19.5.3 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.	2025-07-08	7.8
CVE-2025-47099	adobe - multiple products	InCopy versions 20.3, 19.5.3 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.	2025-07-08	7.8
CVE-2025-47121	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47122	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47123	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47124	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47125	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8

CVE-2025-47126	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47127	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47128	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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.	2025-07-08	7.8
CVE-2025-47129	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47130	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by an Integer Underflow (Wrap or Wraparound) 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.	2025-07-08	7.8
CVE-2025-47131	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47132	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-47133	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 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.	2025-07-08	7.8
CVE-2025-7424	red hat - multiple products	A flaw was found in the libxslt library. The same memory field, psvi, is used for both stylesheet and input data, which can lead to type confusion during XML transformations. This vulnerability allows an attacker to crash the application or corrupt memory. In some cases, it may lead to denial of service or unexpected behavior.	2025-07-10	7.8
CVE-2025-7425	red hat - multiple products	A flaw was found in libxslt where the attribute type, atype, flags are modified in a way that corrupts internal memory management. When XSLT functions, such as the key() process, result in tree fragments, this corruption prevents the proper cleanup of ID attributes. As a result, the system may access freed memory, causing crashes or enabling attackers to trigger heap corruption.	2025-07-10	7.8
CVE-2024-31853	siemens - SICAM TOOLBOX II	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.11). During establishment of a https connection to the TLS server of a managed device, the affected application doesn't check the extended key usage attribute of that device's certificate._x000D_ This could allow an attacker to execute an on-path network (MitM) attack.	2025-07-08	7.7
CVE-2024-31854	siemens - SICAM TOOLBOX II	A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.11). During establishment of a https connection to the TLS server of a managed device, the affected application doesn't check device's certificate common name against an expected value._x000D_ This could allow an attacker to execute an on-path network (MitM) attack.	2025-07-08	7.7
CVE-2025-41224	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM RMC8388 V5.X (All versions < V5.10.0), RUGGEDCOM RMC8388NC V5.X (All versions < V5.10.0), RUGGEDCOM RS416NCv2 V5.X (All versions < V5.10.0), RUGGEDCOM RS416PNCv2 V5.X (All versions < V5.10.0), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.10.0), RUGGEDCOM RS416v2 V5.X (All versions < V5.10.0), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900GNC(32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900NC(32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100NC(32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100P (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100PNC (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2288 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2288NC V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300NC V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300P V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300PNC V5.X (All versions < V5.10.0), RUGGEDCOM RSG2488 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2488NC V5.X (All versions < V5.10.0), RUGGEDCOM RSG907R (All versions < V5.10.0), RUGGEDCOM RSG908C (All versions < V5.10.0), RUGGEDCOM RSG909R (All versions < V5.10.0), RUGGEDCOM RSG910C (All versions < V5.10.0), RUGGEDCOM RSG920P V5.X (All versions < V5.10.0), RUGGEDCOM RSG920PNC V5.X (All versions < V5.10.0), RUGGEDCOM RSL910 (All versions < V5.10.0), RUGGEDCOM RSL910NC (All versions < V5.10.0), RUGGEDCOM RST2228 (All versions < V5.10.0), RUGGEDCOM RST2228P (All versions < V5.10.0), RUGGEDCOM RST916C (All versions < V5.10.0), RUGGEDCOM RST916P (All versions < V5.10.0). The affected products do not properly enforce interface access restrictions when changing from management to non-management interface configurations until a system reboot occurs, despite configuration being saved. This could allow an attacker with network access and credentials to gain access to device through non-management and maintain SSH access to the device until reboot.	2025-07-08	7.7
CVE-2025-53169	huawei - HarmonyOS	Vulnerability of bypassing the process to start SA and use related functions on distributed cameras Impact: Successful exploitation of this vulnerability may allow the peer device to use the camera without user awareness.	2025-07-07	7.6
CVE-2025-21446	qualcomm - fastconnect_6900_firmware	Transient DOS may occur when processing vendor-specific information elements while parsing a WLAN frame for BTM requests.	2025-07-08	7.5
CVE-2025-21449	qualcomm - sm8635p_firmware	Transient DOS may occur while processing malformed length field in SSID IEs.	2025-07-08	7.5
CVE-2025-21454	qualcomm - sa8620p_firmware	Transient DOS while processing received beacon frame.	2025-07-08	7.5

CVE-2025-27057	qualcomm - ar8035_firmware	Transient DOS while handling beacon frames with invalid IE header length.	2025-07-08	7.5
CVE-2025-7345	red hat - multiple products	A flaw exists in gdk-pixbuf within the gdk_pixbuf__jpeg_image_load_increment function (io-jpeg.c) and in glib's g_base64_encode_step (glib/gbase64.c). When processing maliciously crafted JPEG images, a heap buffer overflow can occur during Base64 encoding, allowing out-of-bounds reads from heap memory, potentially causing application crashes or arbitrary code execution.	2025-07-08	7.5
CVE-2025-47984	microsoft - multiple products	Protection mechanism failure in Windows GDI allows an unauthorized attacker to disclose information over a network.	2025-07-08	7.5
CVE-2025-47988	microsoft - Azure Monitor	Improper control of generation of code ('code injection') in Azure Monitor Agent allows an unauthorized attacker to execute code over an adjacent network.	2025-07-08	7.5
CVE-2025-48814	microsoft - multiple products	Missing authentication for critical function in Windows Remote Desktop Licensing Service allows an unauthorized attacker to bypass a security feature over a network.	2025-07-08	7.5
CVE-2025-49716	microsoft - multiple products	Uncontrolled resource consumption in Windows Netlogon allows an unauthorized attacker to deny service over a network.	2025-07-08	7.5
CVE-2025-49718	microsoft - multiple products	Use of uninitialized resource in SQL Server allows an unauthorized attacker to disclose information over a network.	2025-07-08	7.5
CVE-2025-49719	microsoft - multiple products	Improper input validation in SQL Server allows an unauthorized attacker to disclose information over a network.	2025-07-08	7.5
CVE-2024-56468	ibm - InfoSphere Data Replication VSAM for z/OS Remote Source	IBM InfoSphere Data Replication VSAM for z/OS Remote Source 11.4 could allow a remote user to cause a denial of service by sending an invalid HTTP request to the log reading service.	2025-07-08	7.5
CVE-2024-42516	apache software foundation - Apache HTTP Server	HTTP response splitting in the core of Apache HTTP Server allows an attacker who can manipulate the Content-Type response headers of applications hosted or proxied by the server can split the HTTP response. This vulnerability was described as CVE-2023-38709 but the patch included in Apache HTTP Server 2.4.59 did not address the issue. Users are recommended to upgrade to version 2.4.64, which fixes this issue.	2025-07-10	7.5
CVE-2024-43204	apache software foundation - Apache HTTP Server	SSRF in Apache HTTP Server with mod_proxy loaded allows an attacker to send outbound proxy requests to a URL controlled by the attacker. Requires an unlikely configuration where mod_headers is configured to modify the Content-Type request or response header with a value provided in the HTTP request. Users are recommended to upgrade to version 2.4.64 which fixes this issue.	2025-07-10	7.5
CVE-2024-43394	apache software foundation - Apache HTTP Server	Server-Side Request Forgery (SSRF) in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via mod_rewrite or apache expressions that pass unvalidated request input. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.63. Note: The Apache HTTP Server Project will be setting a higher bar for accepting vulnerability reports regarding SSRF via UNC paths. The server offers limited protection against administrators directing the server to open UNC paths. Windows servers should limit the hosts they will connect over via SMB based on the nature of NTLM authentication.	2025-07-10	7.5
CVE-2024-47252	apache software foundation - Apache HTTP Server	Insufficient escaping of user-supplied data in mod_ssl in Apache HTTP Server 2.4.63 and earlier allows an untrusted SSL/TLS client to insert escape characters into log files in some configurations. In a logging configuration where CustomLog is used with "%{varname}x" or "%{varname}c" to log variables provided by mod_ssl such as SSL_TLS_SNI, no escaping is performed by either mod_log_config or mod_ssl and unsanitized data provided by the client may appear in log files.	2025-07-10	7.5
CVE-2025-49630	apache software foundation - Apache HTTP Server	In certain proxy configurations, a denial of service attack against Apache HTTP Server versions 2.4.26 through to 2.4.63 can be triggered by untrusted clients causing an assertion in mod_proxy_http2. Configurations affected are a reverse proxy is configured for an HTTP/2 backend, with ProxyPreserveHost set to "on".	2025-07-10	7.5
CVE-2025-53020	apache software foundation - Apache HTTP Server	Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server. This issue affects Apache HTTP Server: from 2.4.17 up to 2.4.63. Users are recommended to upgrade to version 2.4.64, which fixes the issue.	2025-07-10	7.5
CVE-2025-52434	apache software foundation - Apache Tomcat	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in Apache Tomcat when using the APR/Native connector. This was particularly noticeable with client initiated closes of HTTP/2 connections. This issue affects Apache Tomcat: from 9.0.0.M1 through 9.0.106. Users are recommended to upgrade to version 9.0.107, which fixes the issue.	2025-07-10	7.5
CVE-2025-52520	apache software foundation - Apache Tomcat	For some unlikely configurations of multipart upload, an Integer Overflow vulnerability in Apache Tomcat could lead to a DoS via bypassing of size limits. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0.M1 through 9.0.106. Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.	2025-07-10	7.5

CVE-2025-53506	apache software foundation - Apache Tomcat	Uncontrolled Resource Consumption vulnerability in Apache Tomcat if an HTTP/2 client did not acknowledge the initial settings frame that reduces the maximum permitted concurrent streams. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.8, from 10.1.0-M1 through 10.1.42, from 9.0.0.M1 through 9.0.106. Users are recommended to upgrade to version 11.0.9, 10.1.43 or 9.0.107, which fix the issue.	2025-07-10	7.5
CVE-2024-41169	apache software foundation - Apache Zeppelin	The attacker can use the raft server protocol in an unauthenticated way. The attacker can see the server's resources, including directories and files. This issue affects Apache Zeppelin: from 0.10.1 up to 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue by removing the Cluster Interpreter.	2025-07-12	7.5
CVE-2025-49690	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access Management Service (camsvc) allows an unauthorized attacker to elevate privileges locally.	2025-07-08	7.4
CVE-2025-49538	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an XML Injection vulnerability that could lead to arbitrary file system read. An attacker can exploit this issue by injecting crafted XML or XPath queries to access unauthorized files or lead to denial of service. Exploitation of this issue does not require user interaction, and attack must have access to shared secrets.	2025-07-08	7.4
CVE-2025-49812	apache software foundation - Apache HTTP Server	In some mod_ssl configurations on Apache HTTP Server versions through to 2.4.63, an HTTP desynchronisation attack allows a man-in-the-middle attacker to hijack an HTTP session via a TLS upgrade. Only configurations using "SSLEngine optional" to enable TLS upgrades are affected. Users are recommended to upgrade to version 2.4.64, which removes support for TLS upgrade.	2025-07-10	7.4
CVE-2025-40739	siemens - Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files._x000D_ This could allow an attacker to execute code in the context of the current process.	2025-07-08	7.3
CVE-2025-40740	siemens - Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted PAR files._x000D_ This could allow an attacker to execute code in the context of the current process.	2025-07-08	7.3
CVE-2025-40741	siemens - Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 5). The affected applications contain a stack based overflow vulnerability while parsing specially crafted CFG files._x000D_ This could allow an attacker to execute code in the context of the current process.	2025-07-08	7.3
CVE-2025-49680	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Performance Recorder allows an authorized attacker to deny service locally.	2025-07-08	7.3
CVE-2025-49682	microsoft - multiple products	Use after free in Windows Media allows an authorized attacker to elevate privileges locally.	2025-07-08	7.3
CVE-2025-49536	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized access. Exploitation of this issue does not require user interaction. The vulnerable component is restricted to internal IP addresses.	2025-07-08	7.3
CVE-2025-6759	citrix - Windows Virtual Delivery Agent for CVAD and Citrix DaaS	Local Privilege escalation allows a low-privileged user to gain SYSTEM privileges in Windows Virtual Delivery Agent for CVAD and Citrix DaaS	2025-07-08	7.3
CVE-2025-53650	jenkins - credentials_binding	Jenkins Credentials Binding Plugin 687.v619cb_15e923f and earlier does not properly mask (i.e., replace with asterisks) credentials present in exception error messages that are written to the build log.	2025-07-09	7.3
CVE-2024-52965	fortinet - multiple products	A missing critical step in authentication vulnerability [CWE-304] in Fortinet FortiOS version 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.10, and before 7.0.16 & FortiProxy version 7.6.0 through 7.6.1, 7.4.0 through 7.4.8, 7.2.0 through 7.2.13 and before 7.0.20 allows an API-user using api-key + PKI user certificate authentication to login even if the certificate is invalid.	2025-07-08	7.2
CVE-2025-6770	ivanti - multiple products	OS command injection in Ivanti Endpoint Manager Mobile (EPMM) before version 12.5.0.2 allows a remote authenticated attacker with high privileges to achieve remote code execution	2025-07-08	7.2
CVE-2025-7037	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager before version 2024 SU3 and 2022 SU8 Security Update 1 allows a remote authenticated attacker with admin privileges to read arbitrary data from the database	2025-07-08	7.2
CVE-2025-6771	ivanti - multiple products	OS command injection in Ivanti Endpoint Manager Mobile (EPMM) before version 12.5.0.2,12.4.0.3 and 12.3.0.3 allows a remote authenticated attacker with high privileges to achieve remote code execution	2025-07-08	7.2
CVE-2025-49666	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to execute code over a network.	2025-07-08	7.2
CVE-2025-37102	hewlett packard enterprise (hpe) - HPE Networking Instant On	An authenticated command injection vulnerability exists in the Command line interface of HPE Networking Instant On Access Points. A successful exploitation could allow a remote attacker with elevated privileges to execute arbitrary commands on the underlying operating system as a highly privileged user.	2025-07-08	7.2
CVE-2025-40593	siemens - SIMATIC CN 4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V4.0). The affected application allows to control the device by storing arbitrary files in the SFTP folder of the device. This could allow an attacker to cause a denial of service condition.	2025-07-08	7.1

CVE-2025-21422	qualcomm - aqt1000_firmware	Cryptographic issue while processing crypto API calls, missing checks may lead to corrupted key usage or IV reuses.	2025-07-08	7.1
CVE-2025-48819	microsoft - multiple products	Sensitive data storage in improperly locked memory in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges over an adjacent network.	2025-07-08	7.1
CVE-2025-48821	microsoft - multiple products	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges over an adjacent network.	2025-07-08	7.1
CVE-2025-21006	samsung - android	Out-of-bounds write in handling of macro blocks for MPEG4 codec in libsavsvc.so prior to Android 15 allows local attackers to write out-of-bounds memory.	2025-07-08	7
CVE-2025-7326	microsoft - multiple products	Weak authentication in EOL ASP.NET Core allows an unauthorized attacker to elevate privileges over a network. NOTE: This CVE affects only End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.	2025-07-08	7
CVE-2025-47975	microsoft - multiple products	Double free in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-49677	microsoft - windows_11_22h2	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-49678	microsoft - multiple products	Null pointer dereference in Windows NTFS allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-49685	microsoft - multiple products	Use after free in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-49699	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-07-08	7
CVE-2025-49727	microsoft - multiple products	Heap-based buffer overflow in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-49737	microsoft - Microsoft Teams for Mac	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Teams allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-49744	microsoft - multiple products	Heap-based buffer overflow in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-07-08	7
CVE-2025-53167	huawei - multiple products	Authentication vulnerability in the distributed collaboration framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-07-07	6.9
CVE-2025-23364	siemens - TIA Administrator	A vulnerability has been identified in TIA Administrator (All versions < V3.0.6). The affected application improperly validates code signing certificates._x000D_ This could allow an attacker to bypass the check and exceute arbitrary code during installations.	2025-07-08	6.9
CVE-2025-41222	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM i800 (All versions), RUGGEDCOM i801 (All versions), RUGGEDCOM i802 (All versions), RUGGEDCOM i803 (All versions), RUGGEDCOM M2100 (All versions), RUGGEDCOM M2200 (All versions), RUGGEDCOM M969 (All versions), RUGGEDCOM RMC30 (All versions), RUGGEDCOM RMC8388 V4.X (All versions), RUGGEDCOM RMC8388 V5.X (All versions < V5.10.0), RUGGEDCOM RP110 (All versions), RUGGEDCOM RS1600 (All versions), RUGGEDCOM RS1600F (All versions), RUGGEDCOM RS1600T (All versions), RUGGEDCOM RS400 (All versions), RUGGEDCOM RS401 (All versions), RUGGEDCOM RS416 (All versions), RUGGEDCOM RS416P (All versions), RUGGEDCOM RS416Pv2 V4.X (All versions), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.10.0), RUGGEDCOM RS416v2 V4.X (All versions), RUGGEDCOM RS416v2 V5.X (All versions < V5.10.0), RUGGEDCOM RS8000 (All versions), RUGGEDCOM RS8000A (All versions), RUGGEDCOM RS8000H (All versions), RUGGEDCOM RS8000T (All versions), RUGGEDCOM RS900 (All versions), RUGGEDCOM RS900 (32M) V4.X (All versions), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900G (All versions), RUGGEDCOM RS900G (32M) V4.X (All versions), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900GP (All versions), RUGGEDCOM RS900L (All versions), RUGGEDCOM RS900M-GETS-C01 (All versions), RUGGEDCOM RS900M-GETS-XX (All versions), RUGGEDCOM RS900M-STND-C01 (All versions), RUGGEDCOM RS900M-STND-XX (All versions), RUGGEDCOM RS900W (All versions), RUGGEDCOM RS910 (All versions), RUGGEDCOM RS910L (All versions), RUGGEDCOM RS910W (All versions), RUGGEDCOM RS920L (All versions), RUGGEDCOM RS920W (All versions), RUGGEDCOM RS930L (All versions), RUGGEDCOM RS930W (All versions), RUGGEDCOM RS940G (All versions), RUGGEDCOM RS969 (All versions), RUGGEDCOM RSG2100 (All versions), RUGGEDCOM RSG2100 (32M) V4.X (All versions), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100P (All versions), RUGGEDCOM RSG2100P (32M) V4.X (All versions), RUGGEDCOM RSG2100P (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2200 (All versions), RUGGEDCOM RSG2288 V4.X (All versions), RUGGEDCOM RSG2288 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300 V4.X (All versions), RUGGEDCOM RSG2300 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300P V4.X (All versions), RUGGEDCOM RSG2300P V5.X (All versions < V5.10.0), RUGGEDCOM RSG2488 V4.X (All versions), RUGGEDCOM RSG2488 V5.X (All versions < V5.10.0), RUGGEDCOM RSG907R (All versions < V5.10.0), RUGGEDCOM RSG908C (All versions < V5.10.0), RUGGEDCOM RSG909R (All versions < V5.10.0), RUGGEDCOM RSG910C (All versions < V5.10.0), RUGGEDCOM RSG920P V4.X (All versions), RUGGEDCOM RSG920P V5.X (All versions < V5.10.0), RUGGEDCOM RSL910 (All versions < V5.10.0), RUGGEDCOM RST2228 (All versions < V5.10.0), RUGGEDCOM RST2228P (All versions < V5.10.0), RUGGEDCOM RST916C (All versions < V5.10.0), RUGGEDCOM RST916P (All versions < V5.10.0). Affected devices do not properly handle malformed TLS handshake messages. This could allow an attacker with network access to the webserver to cause a denial of service resulting in the web server and the device to crash.	2025-07-08	6.9
CVE-2025-47999	microsoft - multiple products	Missing synchronization in Windows Hyper-V allows an authorized attacker to deny service over an adjacent network.	2025-07-08	6.8
CVE-2025-48001	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-07-08	6.8
CVE-2025-48003	microsoft - multiple products	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-07-08	6.8

CVE-2025-48800	microsoft - multiple products	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-07-08	6.8
CVE-2025-48804	microsoft - multiple products	Acceptance of extraneous untrusted data with trusted data in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-07-08	6.8
CVE-2025-48818	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-07-08	6.8
CVE-2025-49544	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to access sensitive information or bypass security measures. Exploitation of this issue does not require user interaction and scope is changed.	2025-07-08	6.8
CVE-2024-38327	ibm - Analytics Content Hub	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 is vulnerable to information exposure and further attacks due to an exposed JavaScript source map which could assist an attacker to read and debug JavaScript used in the application's API.	2025-07-10	6.8
CVE-2024-39752	ibm - Analytics Content Hub	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 could be vulnerable to malicious file upload by not validating the type of file uploaded to Explore Content. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks.	2025-07-10	6.8
CVE-2023-39338	ivanti - Sentry	Enables an authenticated user (enrolled device) to access a service protected by Sentry even if they are not authorized according to the sentry policy to access that service. It does not enable the user to authenticate to or use the service, it just provides the tunnel access.	2025-07-12	6.8
CVE-2025-1351	ibm - Storage Virtualize	IBM Storage Virtualize 8.5, 8.6, and 8.7 products could allow a user to escalate their privileges to that of another user logging in at the same time due to a race condition in the login function.	2025-07-07	6.7
CVE-2025-48803	microsoft - multiple products	Missing support for integrity check in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	2025-07-08	6.7
CVE-2025-48811	microsoft - multiple products	Missing support for integrity check in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	2025-07-08	6.7
CVE-2025-53185	huawei - multiple products	Virtual address reuse issue in the memory management module, which can be exploited by non-privileged users to access released memory Impact: Successful exploitation of this vulnerability may affect service integrity.	2025-07-07	6.6
CVE-2025-21426	qualcomm - fastconnect_7800_firmware	Memory corruption while processing camera TPG write request.	2025-07-08	6.6
CVE-2025-0293	ivanti - multiple products	CLRF injection in Ivanti Connect Secure before version 22.7R2.8 and Ivanti Policy Secure before version 22.7R1.5 allows a remote authenticated attacker with admin rights to write to a protected configuration file on disk.	2025-07-08	6.6
CVE-2025-53179	huawei - multiple products	Null pointer dereference vulnerability in the PDF preview module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	6.5
CVE-2025-53180	huawei - multiple products	Null pointer dereference vulnerability in the PDF preview module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	6.5
CVE-2025-53181	huawei - multiple products	Null pointer dereference vulnerability in the PDF preview module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	6.5
CVE-2025-53182	huawei - multiple products	Null pointer dereference vulnerability in the PDF preview module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	6.5
CVE-2025-53183	huawei - multiple products	Null pointer dereference vulnerability in the PDF preview module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	6.5
CVE-2025-53184	huawei - multiple products	Null pointer dereference vulnerability in the PDF preview module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	6.5
CVE-2025-5464	ivanti - multiple products	Insertion of sensitive information into a log file in Ivanti Connect Secure before version 22.7R2.8 allows a local authenticated attacker to obtain that information.	2025-07-08	6.5
CVE-2025-47978	microsoft - multiple products	Out-of-bounds read in Windows Kerberos allows an authorized attacker to deny service over a network.	2025-07-08	6.5
CVE-2025-48802	microsoft - multiple products	Improper certificate validation in Windows SMB allows an authorized attacker to perform spoofing over a network.	2025-07-08	6.5
CVE-2025-49670	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.	2025-07-08	6.5
CVE-2025-49671	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-07-08	6.5
CVE-2025-49681	microsoft - multiple products	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-07-08	6.5
CVE-2025-49706	microsoft - multiple products	Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	2025-07-08	6.5
CVE-2025-7030	drupal - Two-factor Authentication (TFA)	Privilege Defined With Unsafe Actions vulnerability in Drupal Two-factor Authentication (TFA) allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Two-factor Authentication (TFA): from 0.0.0 before 1.11.0.	2025-07-08	6.5
CVE-2025-44526	realtek - rtl8762e_software_development_kit	Realtek RTL8762EKF-EVB RTL8762E SDK V1.4.0 was discovered to utilize insufficient permission checks on critical fields within Bluetooth Low Energy (BLE) data packets. This issue allows attackers to cause a Denial of Service (DoS) via a crafted LL_Length_Req packet.	2025-07-09	6.5
CVE-2025-53654	jenkins - statistics_gatherer	Jenkins Statistics Gatherer Plugin 2.0.3 and earlier stores the AWS Secret Key unencrypted in its global configuration file on the Jenkins controller, where it can be viewed by users with access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53656	jenkins - readyapi_functional_testing	Jenkins ReadyAPI Functional Testing Plugin 1.11 and earlier stores SLM License Access Keys, client secrets, and passwords unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53659	jenkins - qmetry_test_management	Jenkins QMetry Test Management Plugin 1.13 and earlier stores Qmetry Automation API Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5

CVE-2025-53662	jenkins - ifttt_build_notifier	Jenkins IFTTT Build Notifier Plugin 1.2 and earlier stores IFTTT Maker Channel Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53663	jenkins - ibm_cloud_devops	Jenkins IBM Cloud DevOps Plugin 2.0.16 and earlier stores SonarQube authentication tokens unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53664	jenkins - apica_loadtest	Jenkins Apica Loadtest Plugin 1.10 and earlier stores Apica Loadtest LTP authentication tokens unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53666	jenkins - dead_man\'s_snitch	Jenkins Dead Man's Snitch Plugin 0.1 stores Dead Man's Snitch tokens unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53668	jenkins - vaddy	Jenkins VAddy Plugin 1.2.8 and earlier stores Vaddy API Auth Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-53670	jenkins - nouvola_divecloud	Jenkins Nouvola DiveCloud Plugin 1.08 and earlier stores DiveCloud API Keys and Credentials Encryption Keys unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	6.5
CVE-2025-32988	red hat - multiple products	A flaw was found in GnuTLS. A double-free vulnerability exists in GnuTLS due to incorrect ownership handling in the export logic of Subject Alternative Name (SAN) entries containing an otherName. If the type-id OID is invalid or malformed, GnuTLS will call asn1_delete_structure() on an ASN.1 node it does not own, leading to a double-free condition when the parent function or caller later attempts to free the same structure. This vulnerability can be triggered using only public GnuTLS APIs and may result in denial of service or memory corruption, depending on allocator behavior.	2025-07-10	6.5
CVE-2025-32990	red hat - multiple products	A heap-buffer-overflow (off-by-one) flaw was found in the GnuTLS software in the template parsing logic within the certtool utility. When it reads certain settings from a template file, it allows an attacker to cause an out-of-bounds (OOB) NULL pointer write, resulting in memory corruption and a denial-of-service (DoS) that could potentially crash the system.	2025-07-10	6.5
CVE-2025-6395	red hat - multiple products	A NULL pointer dereference flaw was found in the GnuTLS software in _gnutls_figure_common_ciphersuite().	2025-07-10	6.5
CVE-2025-3631	ibm - multiple products	An IBM MQ 9.3 and 9.4 Client connecting to an MQ Queue Manager can cause a SIGSEGV in the AMQRMPPA channel process terminating it.	2025-07-11	6.5
CVE-2025-36104	ibm - Storage Scale	IBM Storage Scale 5.2.3.0 and 5.2.3.1 could allow an authenticated user to obtain sensitive information from files due to the insecure permissions inherited through the SMB protocol.	2025-07-12	6.5
CVE-2025-20982	samsung - multiple products	Out-of-bounds write in setting auth secret in KnoxVault trustlet prior to SMR Jul-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.	2025-07-08	6.4
CVE-2025-20983	samsung - multiple products	Out-of-bounds write in checking auth secret in KnoxVault trustlet prior to SMR Jul-2025 Release 1 allows local privileged attackers to write out-of-bounds memory.	2025-07-08	6.4
CVE-2025-3630	ibm - multiple products	IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.6, 6.2.0.0 through 6.2.0.4, IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6, and 6.2.0.0 through 6.2.0.4 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-07-08	6.4
CVE-2025-41223	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM i800 (All versions), RUGGEDCOM i801 (All versions), RUGGEDCOM i802 (All versions), RUGGEDCOM i803 (All versions), RUGGEDCOM M2100 (All versions), RUGGEDCOM M2200 (All versions), RUGGEDCOM M969 (All versions), RUGGEDCOM RMC30 (All versions), RUGGEDCOM RMC8388 V4.X (All versions), RUGGEDCOM RMC8388 V5.X (All versions < V5.10.0), RUGGEDCOM RP110 (All versions), RUGGEDCOM RS1600 (All versions), RUGGEDCOM RS1600F (All versions), RUGGEDCOM RS1600T (All versions), RUGGEDCOM RS400 (All versions), RUGGEDCOM RS401 (All versions), RUGGEDCOM RS416 (All versions), RUGGEDCOM RS416P (All versions), RUGGEDCOM RS416Pv2 V4.X (All versions), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.10.0), RUGGEDCOM RS416v2 V4.X (All versions), RUGGEDCOM RS416v2 V5.X (All versions < V5.10.0), RUGGEDCOM RS8000 (All versions), RUGGEDCOM RS8000A (All versions), RUGGEDCOM RS8000H (All versions), RUGGEDCOM RS8000T (All versions), RUGGEDCOM RS900 (All versions), RUGGEDCOM RS900 (32M) V4.X (All versions), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900G (All versions), RUGGEDCOM RS900G (32M) V4.X (All versions), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900GP (All versions), RUGGEDCOM RS900L (All versions), RUGGEDCOM RS900M-GETS-C01 (All versions), RUGGEDCOM RS900M-GETS-XX (All versions), RUGGEDCOM RS900M-STND-C01 (All versions), RUGGEDCOM RS900M-STND-XX (All versions), RUGGEDCOM RS900W (All versions), RUGGEDCOM RS910 (All versions), RUGGEDCOM RS910L (All versions), RUGGEDCOM RS910W (All versions), RUGGEDCOM RS920L (All versions), RUGGEDCOM RS920W (All versions), RUGGEDCOM RS930L (All versions), RUGGEDCOM RS930W (All versions), RUGGEDCOM RS940G (All versions), RUGGEDCOM RS969 (All versions), RUGGEDCOM RSG2100 (All versions), RUGGEDCOM RSG2100 (32M) V4.X (All versions), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100P (All versions), RUGGEDCOM RSG2100P (32M) V4.X (All versions), RUGGEDCOM RSG2100P (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2200 (All versions), RUGGEDCOM RSG2288 V4.X (All versions), RUGGEDCOM RSG2288 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300 V4.X (All versions), RUGGEDCOM RSG2300 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300P V4.X (All versions), RUGGEDCOM RSG2300P V5.X (All versions < V5.10.0), RUGGEDCOM RSG2488 V4.X (All versions), RUGGEDCOM RSG2488 V5.X (All versions < V5.10.0), RUGGEDCOM RSG907R (All versions < V5.10.0), RUGGEDCOM RSG908C (All versions < V5.10.0), RUGGEDCOM RSG909R (All versions < V5.10.0), RUGGEDCOM RSG910C (All versions < V5.10.0), RUGGEDCOM RSG920P V4.X (All versions), RUGGEDCOM RSG920P V5.X (All versions < V5.10.0), RUGGEDCOM RSL910 (All versions < V5.10.0),	2025-07-08	6.3

		RUGGEDCOM RST2228 (All versions < V5.10.0), RUGGEDCOM RST2228P (All versions < V5.10.0), RUGGEDCOM RST916C (All versions < V5.10.0), RUGGEDCOM RST916P (All versions < V5.10.0). The affected devices support the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 cipher suite, which uses CBC (Cipher Block Chaining) mode that is known to be vulnerable to timing attacks. This could allow an attacker to compromise the integrity and confidentiality of encrypted communications.		
CVE-2025-5450	ivanti - multiple products	Improper access control in the certificate management component of Ivanti Connect Secure before version 22.7R2.8 and Ivanti Policy Secure before version 22.7R1.5 allows a remote authenticated admin with read-only rights to modify settings that should be restricted.	2025-07-08	6.3
CVE-2025-53651	jenkins - html_publisher	Jenkins HTML Publisher Plugin 425 and earlier displays log messages that include the absolute paths of files archived during the Publish HTML reports post-build step, exposing information about the Jenkins controller file system in the build log.	2025-07-09	6.3
CVE-2025-47963	microsoft - edge_chromium	No cwe for this issue in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2025-07-11	6.3
CVE-2025-21000	samsung - multiple products	Improper privilege management in Bluetooth prior to SMR Jul-2025 Release 1 allows local attackers to enable Bluetooth.	2025-07-08	6.2
CVE-2025-21001	samsung - multiple products	Improper access control in LeAudioService prior to SMR Jul-2025 Release 1 allows local attackers to stop broadcasting Auracast.	2025-07-08	6.2
CVE-2025-21002	samsung - multiple products	Improper access control in LeAudioService prior to SMR Jul-2025 Release 1 allows local attackers to manipulate broadcasting Auracast.	2025-07-08	6.2
CVE-2025-21433	qualcomm - apq8017_firmware	Transient DOS when importing a PKCS#8-encoded RSA private key with a zero-sized modulus.	2025-07-08	6.2
CVE-2025-47980	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Imaging Component allows an unauthorized attacker to disclose information locally.	2025-07-08	6.2
CVE-2025-49545	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A high-privilege authenticated attacker can force the application to make arbitrary requests via injection of URLs. Exploitation of this issue does not require user interaction and scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	6.2
CVE-2025-6044	google - ChromeOS	An Improper Access Control vulnerability in the Stylus Tools component of Google ChromeOS version 16238.64.0 on the garaged stylus devices allows a physical attacker to bypass the lock screen and access user files by removing the stylus while the device is closed and using the screen capture feature.	2025-07-07	6.1
CVE-2023-52236	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM i800 (All versions), RUGGEDCOM i801 (All versions), RUGGEDCOM i802 (All versions), RUGGEDCOM i803 (All versions), RUGGEDCOM M2100 (All versions), RUGGEDCOM M2200 (All versions), RUGGEDCOM M969 (All versions), RUGGEDCOM RMC30 (All versions), RUGGEDCOM RMC8388 V4.X (All versions), RUGGEDCOM RMC8388 V5.X (All versions < V5.10.0), RUGGEDCOM RP110 (All versions), RUGGEDCOM RS1600 (All versions), RUGGEDCOM RS1600F (All versions), RUGGEDCOM RS1600T (All versions), RUGGEDCOM RS400 (All versions), RUGGEDCOM RS401 (All versions), RUGGEDCOM RS416 (All versions), RUGGEDCOM RS416P (All versions), RUGGEDCOM RS416Pv2 V4.X (All versions), RUGGEDCOM RS416Pv2 V5.X (All versions < V5.10.0), RUGGEDCOM RS416v2 V4.X (All versions), RUGGEDCOM RS416v2 V5.X (All versions < V5.10.0), RUGGEDCOM RS8000 (All versions), RUGGEDCOM RS8000A (All versions), RUGGEDCOM RS8000H (All versions), RUGGEDCOM RS8000T (All versions), RUGGEDCOM RS900 (All versions), RUGGEDCOM RS900 (32M) V4.X (All versions), RUGGEDCOM RS900 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900G (All versions), RUGGEDCOM RS900G (32M) V4.X (All versions), RUGGEDCOM RS900G (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RS900GP (All versions), RUGGEDCOM RS900L (All versions), RUGGEDCOM RS900M-GETS-C01 (All versions), RUGGEDCOM RS900M-GETS-XX (All versions), RUGGEDCOM RS900M-STND-C01 (All versions), RUGGEDCOM RS900M-STND-XX (All versions), RUGGEDCOM RS900W (All versions), RUGGEDCOM RS910 (All versions), RUGGEDCOM RS910L (All versions), RUGGEDCOM RS910W (All versions), RUGGEDCOM RS920L (All versions), RUGGEDCOM RS920W (All versions), RUGGEDCOM RS930L (All versions), RUGGEDCOM RS930W (All versions), RUGGEDCOM RS940G (All versions), RUGGEDCOM RS969 (All versions), RUGGEDCOM RSG2100 (All versions), RUGGEDCOM RSG2100 (32M) V4.X (All versions), RUGGEDCOM RSG2100 (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2100P (All versions), RUGGEDCOM RSG2100P (32M) V4.X (All versions), RUGGEDCOM RSG2100P (32M) V5.X (All versions < V5.10.0), RUGGEDCOM RSG2200 (All versions), RUGGEDCOM RSG2288 V4.X (All versions), RUGGEDCOM RSG2288 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300 V4.X (All versions), RUGGEDCOM RSG2300 V5.X (All versions < V5.10.0), RUGGEDCOM RSG2300P V4.X (All versions), RUGGEDCOM RSG2300P V5.X (All versions < V5.10.0), RUGGEDCOM RSG2488 V4.X (All versions), RUGGEDCOM RSG2488 V5.X (All versions < V5.10.0), RUGGEDCOM RSG907R (All versions < V5.10.0), RUGGEDCOM RSG908C (All versions < V5.10.0), RUGGEDCOM RSG909R (All versions < V5.10.0), RUGGEDCOM RSG910C (All versions < V5.10.0), RUGGEDCOM RSG920P V4.X (All versions), RUGGEDCOM RSG920P V5.X (All versions < V5.10.0), RUGGEDCOM RSL910 (All versions < V5.10.0), RUGGEDCOM RST2228 (All versions < V5.10.0), RUGGEDCOM RST2228P (All versions < V5.10.0), RUGGEDCOM RST916C (All versions < V5.10.0), RUGGEDCOM RST916P (All versions < V5.10.0). The affected products support insecure cryptographic algorithms. An attacker could leverage these legacy algorithms to achieve a man-in-the-middle attack or impersonate communicating parties.	2025-07-08	6.1
CVE-2023-43039	ibm - openpages_with_watson	IBM OpenPages with Watson 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session	2025-07-08	6.1
CVE-2025-40742	siemens - multiple products	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions), SIPROTEC 5 6MD89 (CP300) (All versions), SIPROTEC 5 6MD89 (CP300) V9.6 (All versions), SIPROTEC 5 6MU85 (CP300) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions), SIPROTEC 5 7SJ81 (CP100) (All versions), SIPROTEC 5 7SJ81 (CP150) (All versions), SIPROTEC 5 7SJ82 (CP100) (All	2025-07-08	6

		versions), SIPROTEC 5 7SJ82 (CP150) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions), SIPROTEC 5 7SK82 (CP100) (All versions), SIPROTEC 5 7SK82 (CP150) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions), SIPROTEC 5 7ST86 (CP300) (All versions), SIPROTEC 5 7SX82 (CP150) (All versions), SIPROTEC 5 7SX85 (CP300) (All versions), SIPROTEC 5 7SY82 (CP150) (All versions), SIPROTEC 5 7UM85 (CP300) (All versions), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions), SIPROTEC 5 7VE85 (CP300) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions), SIPROTEC 5 7VU85 (CP300) (All versions), SIPROTEC 5 Compact 7SX800 (CP050) (All versions). The affected devices include session identifiers in URL requests for certain functionalities. This could allow an attacker to retrieve sensitive session data from browser history, logs, or other storage mechanisms, potentially leading to unauthorized access.		
CVE-2025-21195	microsoft - multiple products	Improper link resolution before file access ('link following') in Service Fabric allows an authorized attacker to elevate privileges locally.	2025-07-08	6
CVE-2025-53186	huawei - multiple products	Vulnerability that allows third-party call apps to send broadcasts without verification in the audio framework module Impact: Successful exploitation of this vulnerability may affect availability.	2025-07-07	5.9
CVE-2024-43190	ibm - Engineering Requirements Management DOORS	IBM Engineering Requirements Management DOORS 9.7.2.9, under certain configurations, could allow a remote attacker to obtain password reset instructions of a legitimate user using man in the middle techniques.	2025-07-07	5.9
CVE-2025-48823	microsoft - multiple products	Cryptographic issues in Windows Cryptographic Services allows an unauthorized attacker to disclose information over a network.	2025-07-08	5.9
CVE-2025-53168	huawei - HarmonyOS	Vulnerability of bypassing the process to start SA and use related functions on distributed cameras Impact: Successful exploitation of this vulnerability may allow the peer device to use the camera without user awareness.	2025-07-07	5.7
CVE-2025-48002	microsoft - multiple products	Integer overflow or wraparound in Windows Hyper-V allows an authorized attacker to disclose information over an adjacent network.	2025-07-08	5.7
CVE-2025-49722	microsoft - multiple products	Uncontrolled resource consumption in Windows Print Spooler Components allows an authorized attacker to deny service over an adjacent network.	2025-07-08	5.7
CVE-2024-38648	ivanti - desktop_\&_server_management	A hardcoded secret in Ivanti DSM before 2024.2 allows an authenticated attacker on an adjacent network to decrypt sensitive data including user credentials.	2025-07-12	5.7
CVE-2025-47182	microsoft - edge_chromium	Improper input validation in Microsoft Edge (Chromium-based) allows an authorized attacker to bypass a security feature locally.	2025-07-11	5.6
CVE-2025-21005	samsung - android	Improper access control in isemtelephony prior to Android 15 allows local attackers to access sensitive information.	2025-07-08	5.5
CVE-2025-21007	samsung - android	Out-of-bounds write in accessing uninitialized memory in libsavsvc.so prior to Android 15 allows local attackers to cause memory corruption.	2025-07-08	5.5
CVE-2025-21008	samsung - android	Out-of-bounds read in decoding frame header in libsavsvc.so prior to Android 15 allows local attackers to cause memory corruption.	2025-07-08	5.5
CVE-2025-21009	samsung - android	Out-of-bounds read in decoding malformed frame header in libsavsvc.so prior to Android 15 allows local attackers to cause memory corruption.	2025-07-08	5.5
CVE-2025-5463	ivanti - multiple products	Insertion of sensitive information into a log file in Ivanti Connect Secure before version 22.7R2.8 and Ivanti Policy Secure before version 22.7R1.5 allows a local authenticated attacker to obtain that information.	2025-07-08	5.5
CVE-2025-0292	ivanti - multiple products	SSRF in Ivanti Connect Secure before version 22.7R2.8 and Ivanti Policy Secure before version 22.7R1.5 allows a remote authenticated attacker with admin rights to access internal network services.	2025-07-08	5.5
CVE-2025-21167	adobe - substance_3d_designer	Substance3D - Designer versions 14.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-21168	adobe - substance_3d_designer	Substance3D - Designer versions 14.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-26636	microsoft - multiple products	Processor optimization removal or modification of security-critical code in Windows Kernel allows an authorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-43580	adobe - multiple products	Audition versions 25.2, 24.6.3 and earlier are affected by an Access of Memory Location After End of Buffer vulnerability that could result in application denial-of-service. An attacker could leverage this vulnerability to crash the application or disrupt its functionality. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-43587	adobe - multiple products	After Effects versions 25.2, 24.6.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-47109	adobe - multiple products	After Effects versions 25.2, 24.6.6 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption to services. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-48808	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-48809	microsoft - multiple products	Processor optimization removal or modification of security-critical code in Windows Kernel allows an authorized attacker to disclose information locally.	2025-07-08	5.5

CVE-2025-48810	microsoft - multiple products	Processor optimization removal or modification of security-critical code in Windows Secure Kernel Mode allows an authorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-48812	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-49658	microsoft - multiple products	Out-of-bounds read in Windows TDX.sys allows an authorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-49664	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows User-Mode Driver Framework Host allows an authorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-49684	microsoft - multiple products	Buffer over-read in Storage Port Driver allows an authorized attacker to disclose information locally.	2025-07-08	5.5
CVE-2025-47135	adobe - dimension	Dimension versions 4.1.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-43583	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.22 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application, causing disruption in service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-07-08	5.5
CVE-2025-43584	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.22 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.	2025-07-08	5.5
CVE-2025-27165	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.2 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.	2025-07-08	5.5
CVE-2025-30313	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	5.5
CVE-2025-49524	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this 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.	2025-07-08	5.5
CVE-2025-49525	adobe - multiple products	Illustrator versions 28.7.6, 29.5.1 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.	2025-07-08	5.5
CVE-2025-47119	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to application denial-of-service. An attacker could exploit this 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.	2025-07-08	5.5
CVE-2025-47120	adobe - multiple products	Adobe Framemaker versions 2020.8, 2022.6 and earlier are affected by a Stack-based Buffer Overflow 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.	2025-07-08	5.5
CVE-2025-2793	ibm - multiple products	IBM Sterling B2B Integrator 6.0.0.0 through 6.1.2.6, 6.2.0.0 through 6.2.0.4, IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6, and 6.2.0.0 through 6.2.0.4 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.	2025-07-08	5.4
CVE-2025-49534	adobe - experience_manager	Adobe Experience Manager versions 11.4 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2025-07-08	5.4
CVE-2025-49547	adobe - experience_manager	Adobe Experience Manager versions 11.4 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2025-07-08	5.4
CVE-2025-53658	jenkins - applitools_eyes	Jenkins Applitools Eyes Plugin 1.16.5 and earlier does not escape the Applitools URL on the build page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2025-07-09	5.4
CVE-2025-7365	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak. When an authenticated attacker attempts to merge accounts with another existing account during an identity provider (IdP) login, the attacker will subsequently be prompted to "review profile" information. This vulnerability allows the attacker to modify their email address to match that of a victim's account, triggering a verification email sent to the victim's email address. The attacker's email address is not present in the verification email content, making it a potential phishing opportunity. If the victim clicks the verification link, the attacker can gain access to the victim's account.	2025-07-10	5.4
CVE-2025-47964	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2025-07-11	5.4
CVE-2025-53173	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	5.3
CVE-2025-27127	siemens - multiple products	A vulnerability has been identified in TIA Project-Server (All versions < V2.1.1), TIA Project-Server V17 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions), Totally Integrated Automation Portal (TIA Portal) V18 (All versions), Totally Integrated Automation Portal (TIA Portal) V19 (All versions), Totally Integrated Automation Portal (TIA Portal) V20 (All versions < V20 Update 3). The affected application improperly handles uploaded projects in the document	2025-07-08	5.3

		root. This could allow an attacker with contributor privileges to cause denial of service by uploading a malicious project.		
CVE-2024-53009	qualcomm - aqt1000_firmware	Memory corruption while operating the mailbox in Automotive.	2025-07-08	5.3
CVE-2024-55599	fortinet - multiple products	An Improperly Implemented Security Check for Standard vulnerability [CWE-358] in FortiOS version 7.6.0, version 7.4.7 and below, 7.0 all versions, 6.4 all versions and FortiProxy version 7.6.1 and below, version 7.4.8 and below, 7.2 all versions, 7.0 all versions may allow a remote unauthenticated user to bypass the DNS filter via Apple devices.	2025-07-08	5.3
CVE-2024-49783	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in storage of encrypted data. If an authenticated remote attacker with access to the database or a local attacker with access to server files could extract the encrypted data, they could exploit this vulnerability to use additional cryptographic methods to possibly extract the encrypted data.	2025-07-08	5.3
CVE-2024-49784	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 could provide weaker than expected security in storage of encrypted data with AES encryption and CBC mode. If an authenticated remote attacker with access to the database or a local attacker with access to server files could extract the encrypted data values they could exploit this weaker algorithm to use additional cryptographic methods to possibly extract the encrypted data.	2025-07-08	5.3
CVE-2025-27367	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 is vulnerable to improper input validation due to bypassing of client-side validation for the data types and requiredness of fields for GRC Objects when an authenticated user sends a specially crafted payload to the server allowing for data to be saved without storing the required fields.	2025-07-08	5.3
CVE-2025-7031	drupal - Config Pages Viewer	Missing Authentication for Critical Function vulnerability in Drupal Config Pages Viewer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Config Pages Viewer: from 0.0.0 before 1.0.4.	2025-07-08	5.3
CVE-2025-53655	jenkins - statistics_gatherer	Jenkins Statistics Gatherer Plugin 2.0.3 and earlier does not mask the AWS Secret Key on the global configuration form, increasing the potential for attackers to observe and capture it.	2025-07-09	5.3
CVE-2025-53667	jenkins - dead_man\'s_snitch	Jenkins Dead Man's Snitch Plugin 0.1 does not mask Dead Man's Snitch tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2025-07-09	5.3
CVE-2025-32989	red hat - multiple products	A heap-buffer-overread vulnerability was found in GnuTLS in how it handles the Certificate Transparency (CT) Signed Certificate Timestamp (SCT) extension during X.509 certificate parsing. This flaw allows a malicious user to create a certificate containing a malformed SCT extension (OID 1.3.6.1.4.1.11129.2.4.2) that contains sensitive data. This issue leads to the exposure of confidential information when GnuTLS verifies certificates from certain websites when the certificate (SCT) is not checked correctly.	2025-07-10	5.3
CVE-2025-7407	netgear - d6400_firmware	A vulnerability, which was classified as critical, was found in Netgear D6400 1.0.0.114. This affects an unknown part of the file diag.cgi. The manipulation of the argument host_name leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early and confirmed the existence of the vulnerability. They reacted very quickly, professional and kind. This vulnerability only affects products that are no longer supported by the maintainer.	2025-07-10	5.3
CVE-2024-37524	ibm - Analytics Content Hub	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser.	2025-07-10	5.3
CVE-2025-48924	apache software foundation - multiple products	Uncontrolled Recursion vulnerability in Apache Commons Lang. This issue affects Apache Commons Lang: Starting with commons-lang:commons-lang 2.0 to 2.6, and, from org.apache.commons:commons-lang3 3.0 before 3.18.0. The methods ClassUtils.getClass(...) can throw StackOverflowError on very long inputs. Because an Error is usually not handled by applications and libraries, a StackOverflowError could cause an application to stop. Users are recommended to upgrade to version 3.18.0, which fixes the issue.	2025-07-11	5.3
CVE-2025-49542	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an unauthenticated attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser, scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	5.2
CVE-2025-5987	red hat - multiple products	A flaw was found in libssh when using the ChaCha20 cipher with the OpenSSL library. If an attacker manages to exhaust the heap space, this error is not detected and may lead to libssh using a partially initialized cipher context. This occurs because the OpenSSL error code returned aliases with the SSH_OK code, resulting in libssh not properly detecting the error returned by the OpenSSL library. This issue can lead to undefined behavior, including compromised data confidentiality and integrity or crashes.	2025-07-07	5
CVE-2025-5451	ivanti - multiple products	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.8 and Ivanti Policy Secure before version 22.7R1.5 allows a remote authenticated attacker with admin rights to trigger a denial of service.	2025-07-08	4.9
CVE-2023-39339	ivanti - multiple products	A vulnerability exists on all versions of Ivanti Policy Secure below 22.6R1 where an authenticated administrator can perform an arbitrary file read via a maliciously crafted web request.	2025-07-12	4.9

CVE-2025-53178	huawei - multiple products	Permission bypass vulnerability in the calendar storage module Impact: Successful exploitation of this vulnerability may affect the schedule reminder function of head units.	2025-07-07	4.8
CVE-2025-31267	apple - App Store Connect	An authentication issue was addressed with improved state management. This issue is fixed in App Store Connect 3.0. An attacker with physical access to an unlocked device may be able to view sensitive user information.	2025-07-10	4.6
CVE-2025-49539	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in a security feature bypass. A high-privileged attacker could leverage this vulnerability to access sensitive information. Exploitation of this issue does not require user interaction. The vulnerable component is restricted to internal IP addresses.	2025-07-08	4.5
CVE-2025-2827	ibm - Sterling File Gateway	IBM Sterling File Gateway 6.0.0.0 through 6.1.2.6, and 6.2.0.0 through 6.2.0.4 could disclose sensitive installation directory information to an authenticated user that could be used in further attacks against the system.	2025-07-08	4.3
CVE-2025-27369	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 is vulnerable to information disclosure of sensitive information due to a weaker than expected security for certain REST end points used for the administration of OpenPages. An authenticated user is able to obtain certain information about system configuration and internal state which is only intended for administrators of the system.	2025-07-08	4.3
CVE-2025-49540	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	4.3
CVE-2025-49541	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	4.3
CVE-2025-49543	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, scope is changed. The vulnerable component is restricted to internal IP addresses.	2025-07-08	4.3
CVE-2025-1112	ibm - multiple products	IBM OpenPages with Watson 8.3 and 9.0 could allow an authenticated user to obtain sensitive information that should only be available to privileged users.	2025-07-09	4.3
CVE-2025-2670	ibm - OpenPages	IBM OpenPages 9.0 is vulnerable to information disclosure of sensitive information due to a weaker than expected security for certain REST end points related to workflow feature of OpenPages. An authenticated user is able to obtain certain information about Workflow related configuration and internal state.	2025-07-09	4.3
CVE-2025-53653	jenkins - aqua_security_scanner	Jenkins Aqua Security Scanner Plugin 3.2.8 and earlier stores Scanner Tokens for Aqua API unencrypted in job config.xml files on the Jenkins controller, where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2025-07-09	4.3
CVE-2025-53657	jenkins - readyapi_functional_testing	Jenkins ReadyAPI Functional Testing Plugin 1.11 and earlier does not mask SLM License Access Keys, client secrets, and passwords displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2025-07-09	4.3
CVE-2025-53660	jenkins - qmetry_test_management	Jenkins QMetry Test Management Plugin 1.13 and earlier does not mask Qmetry Automation API Keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2025-07-09	4.3
CVE-2025-53661	jenkins - testsigma_test_plan_run	Jenkins Testsigma Test Plan run Plugin 1.6 and earlier does not mask Testsigma API keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2025-07-09	4.3
CVE-2025-53665	jenkins - apica_loadtest	Jenkins Apica Loadtest Plugin 1.10 and earlier does not mask Apica Loadtest LTP authentication tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2025-07-09	4.3
CVE-2025-53669	jenkins - vaddy	Jenkins VAddy Plugin 1.2.8 and earlier does not mask Vaddy API Auth Keys displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	2025-07-09	4.3
CVE-2025-36599	dell - PowerFlex Manager VM	Dell PowerFlex Manager VM, versions prior to 4.6.2.1, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account.	2025-07-09	4.3
CVE-2025-36090	ibm - Analytics Content Hub	IBM Analytics Content Hub 2.0, 2.1, 2.2, and 2.3 could allow a remote attacker to obtain information about the application framework which could be used in reconnaissance to gather information for future attacks from a detailed technical error message.	2025-07-10	4.3

CVE-2025-20999	samsung - multiple products	Improper authorization in accessing saved Wi-Fi password for Galaxy Tablet prior to SMR Jul-2025 Release 1 allows secondary users to access owner's saved Wi-Fi password.	2025-07-08	4.1
CVE-2025-45582	gnu - tar	GNU Tar through 1.35 allows file overwrite via directory traversal in crafted TAR archives, with a certain two-step process. First, the victim must extract an archive that contains a ../ symlink to a critical directory. Second, the victim must extract an archive that contains a critical file, specified via a relative pathname that begins with the symlink name and ends with that critical file's name. Here, the extraction follows the symlink and overwrites the critical file. This bypasses the protection mechanism of "Member name contains '..'" that would occur for a single TAR archive that attempted to specify the critical file via a ../ approach. For example, the first archive can contain "x -> ../../../../home/victim/.ssh" and the second archive can contain x/authorized_keys. This can affect server applications that automatically extract any number of user-supplied TAR archives, and were relying on the blocking of traversal. This can also affect software installation processes in which "tar xf" is run more than once (e.g., when installing a package can automatically install two dependencies that are set up as untrusted tarballs instead of official packages).	2025-07-11	4.1
CVE-2024-58117	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	4
CVE-2025-53170	huawei - harmonyos	Null pointer dereference vulnerability in the application exit cause module Impact: Successful exploitation of this vulnerability may affect function stability.	2025-07-07	4
CVE-2025-53171	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	4
CVE-2025-53172	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	4
CVE-2025-53174	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	4
CVE-2025-53175	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	4
CVE-2025-21003	samsung - multiple products	Insecure storage of sensitive information in Emergency SOS prior to SMR Jul-2025 Release 1 allows local attackers to access sensitive information.	2025-07-08	4
CVE-2025-53177	huawei - multiple products	Permission bypass vulnerability in the calendar storage module Impact: Successful exploitation of this vulnerability may affect the schedule syncing function of watches.	2025-07-07	3.9
CVE-2025-49760	microsoft - multiple products	External control of file name or path in Windows Storage allows an authorized attacker to perform spoofing over a network.	2025-07-08	3.5
CVE-2025-53862	red hat - multiple products	A flaw was found in Ansible. Three API endpoints are accessible and return verbose, unauthenticated responses. This flaw allows a malicious user to access data that may contain important information.	2025-07-11	3.5
CVE-2025-53176	huawei - multiple products	Stack overflow risk when vector images are parsed during file preview Impact: Successful exploitation of this vulnerability may affect the file preview function.	2025-07-07	3.3
CVE-2025-49756	microsoft - Microsoft 365 Apps for Enterprise	Use of a broken or risky cryptographic algorithm in Office Developer Platform allows an authorized attacker to bypass a security feature locally.	2025-07-08	3.3
CVE-2025-49731	microsoft - multiple products	Improper handling of insufficient permissions or privileges in Microsoft Teams allows an authorized attacker to elevate privileges over a network.	2025-07-08	3.1
CVE-2025-53861	red hat - Red Hat Ansible Automation Platform 2	A flaw was found in Ansible. Sensitive cookies without security flags over non-encrypted channels can lead to Man-in-the-Middle (MitM) and Cross-site scripting (XSS) attacks allowing attackers to read transmitted data.	2025-07-11	3.1
CVE-2025-24474	fortinet - multiple products	An Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability [CWE-89] in FortiManager 7.6.0 through 7.6.1, 7.4.0 through 7.4.6, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiManager Cloud 7.4.1 through 7.4.6, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiAnalyzer 7.6.0 through 7.6.1, 7.4.0 through 7.4.6, 7.2 all versions, 7.0 all versions, 6.4 all versions; and FortiAnalyzer Cloud 7.4.1 through 7.4.6, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow an authenticated attacker with high privilege to extract database information via crafted requests.	2025-07-08	2.7
CVE-2025-49546	adobe - multiple products	ColdFusion versions 2025.2, 2023.14, 2021.20 and earlier are affected by an Improper Access Control vulnerability that could lead to a partial application denial-of-service. A high-privileged attacker could exploit this vulnerability to partially disrupt the availability of the application. Exploitation of this issue does not require user interaction and scope is unchanged. The vulnerable component is restricted to internal IP addresses.	2025-07-08	2.4

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.