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 7th of September to 12th of September. 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 7 سبتمبر إلى 12 سبتمبر. 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-2025-55232	microsoft - Microsoft HPC Pack 2019	Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) allows an unauthorized attacker to execute code over a network.	2025-09-09	9.8
CVE-2025-10159	sophos - AP6 Series Wireless Access Points	An authentication bypass vulnerability allows remote attackers to gain administrative privileges on Sophos AP6 Series Wireless Access Points older than firmware version 1.7.2563 (MR7).	2025-09-09	9.8
CVE-2025-40795	siemens - multiple products	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a stack-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.	2025-09-09	9.3
CVE-2025-40804	siemens - SIMATIC Virtualization as a Service (SIVaaS)	A vulnerability has been identified in SIMATIC Virtualization as a Service (SIVaaS) (All versions). The affected application exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.	2025-09-09	9.3
CVE-2025-54236	adobe - multiple products	Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Improper Input Validation vulnerability. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high. Exploitation of this issue does not require user interaction.	2025-09-09	9.1
CVE-2025-54261	adobe - multiple products	ColdFusion versions 2025.3, 2023.15, 2021.21 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary code execution by an attacker. Scope is changed.	2025-09-09	9.0
CVE-2025-55145	ivanti - multiple products	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker to hijack existing HTML5 connections.	2025-09-09	8.9
CVE-2025-36855	microsoft - .NET 6.0	A vulnerability (CVE-2025-21176 https://www.cve.org/CVERecord) exists in DiaSymReader.dll due to buffer over-read. Per CWE-126: Buffer Over-read https://cwe.mitre.org/data/definitions/126.html , Buffer Over-read is when a product reads from a buffer using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer. This issue affects EOL ASP.NET 6.0.0 <= 6.0.36 as represented in this CVE, as well as 8.0.0 <= 8.0.11 & <= 9.0.0 as represented in CVE-2025-21176. Additionally, if you've deployed self-contained applications https://docs.microsoft.com/dotnet/core/deploying/#self-contained-deployments-scd targeting any of the impacted versions, these applications are also vulnerable and must be recompiled and redeployed. 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.	2025-09-08	8.8
CVE-2025-24404	apache - hertzbeat	XML Injection RCE by parse http sitemap xml response vulnerability in Apache HertzBeat.	2025-09-09	8.8

		The attacker needs to have an authenticated account with access, and add monitor parsed by xml, returned special content can trigger the XML parsing vulnerability. This issue affects Apache HertzBeat (incubating): before 1.7.0. Users are recommended to upgrade to version 1.7.0, which fixes the issue.		
CVE-2025-48208	apache - hertzbeat	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in Apache HertzBeat . The attacker needs to have an authenticated account with access, and the attack can only be triggered by crafting custom commands. A successful attack would result in arbitrary script execution. This issue affects Apache HertzBeat: through 1.7.2. Users are recommended to upgrade to version [1.7.3], which fixes the issue.	2025-09-09	8.8
CVE-2025-55141	ivanti - multiple products	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure authentication related settings.	2025-09-09	8.8
CVE-2025-55142	ivanti - multiple products	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure authentication related settings.	2025-09-09	8.8
CVE-2025-55147	ivanti - multiple products	CSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to execute sensitive actions on behalf of the victim user. User interaction is required	2025-09-09	8.8
CVE-2025-9712	ivanti - Endpoint Manager	Insufficient filename validation in Ivanti Endpoint Manager before 2024 SU3 SR1 and 2022 SU8 SR2 allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	2025-09-09	8.8
CVE-2025-9872	ivanti - Endpoint Manager	Insufficient filename validation in Ivanti Endpoint Manager before 2024 SU3 SR1 and 2022 SU8 SR2 allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	2025-09-09	8.8
CVE-2025-54106	microsoft - multiple products	Integer overflow or wraparound in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	2025-09-09	8.8
CVE-2025-54110	microsoft - multiple products	Integer overflow or wraparound in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-09-09	8.8
CVE-2025-54113	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.	2025-09-09	8.8
CVE-2025-54897	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-09-09	8.8
CVE-2025-54918	microsoft - multiple products	Improper authentication in Windows NTLM allows an authorized attacker to elevate privileges over a network.	2025-09-09	8.8
CVE-2025-55227	microsoft - multiple products	Improper neutralization of special elements used in a command ('command injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2025-09-09	8.8
CVE-2025-55234	microsoft - multiple products	SMB Server might be susceptible to relay attacks depending on the configuration. An attacker who successfully exploited these vulnerabilities could perform relay attacks and make the users subject to elevation of privilege attacks. The SMB Server already supports mechanisms for hardening against relay attacks: SMB Server signing SMB Server Extended Protection for Authentication (EPA) Microsoft is releasing this CVE to provide customers with audit capabilities to help them to assess their environment and to identify any potential device or software incompatibility issues before deploying SMB Server hardening measures that protect against relay attacks.	2025-09-09	8.8

		If you have not already enabled SMB Server hardening measures, we advise customers to take the following actions to be protected from these relay attacks: Assess your environment by utilizing the audit capabilities that we are exposing in the September 2025 security updates. See Support for Audit Events to deploy SMB Server Hardening—SMB Server Signing &amp; SMB Server EPA. Adopt appropriate SMB Server hardening measures.		
CVE-2025-43888	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, Hyper-V, version(s) 19.19 and 19.20, contain(s) an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2025-09-10	8.8
CVE-2025-10200	google - chrome	Use after free in Serviceworker in Google Chrome on Desktop prior to 140.0.7339.127 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2025-09-10	8.8
CVE-2025-10201	google - chrome	Inappropriate implementation in Mojo in Google Chrome on Android, Linux, ChromeOS prior to 140.0.7339.127 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2025-09-10	8.8
CVE-2025-55319	microsoft - visual_studio_code	Ai command injection in Agentic AI and Visual Studio Code allows an unauthorized attacker to execute code over a network.	2025-09-12	8.8
CVE-2025-21042	samsung - multiple products	Out-of-bounds write in libimagecodec.quram.so prior to SMR Apr-2025 Release 1 allows remote attackers to execute arbitrary code.	2025-09-12	8.8
CVE-2025-21043	samsung - multiple products	Out-of-bounds write in libimagecodec.quram.so prior to SMR Sep-2025 Release 1 allows remote attackers to execute arbitrary code.	2025-09-12	8.8
CVE-2025-40796	siemens - multiple products	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	2025-09-09	8.7
CVE-2025-40797	siemens - multiple products	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	2025-09-09	8.7
CVE-2025-40798	siemens - multiple products	A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.	2025-09-09	8.7
CVE-2025-8557	lenovo - XClarity Orchestrator (LXCO)	An internal product security audit of Lenovo XClarity Orchestrator (LXCO) discovered the below vulnerability: An attacker with access to a device on the local Lenovo XClarity Orchestrator (LXCO) network segment may be able to manipulate the local device to create an alternate communication channel which could allow the attacker, under certain conditions, to directly interact with backend LXCO API services typically inaccessible to users. While access controls may limit the scope of interaction, this could result in unauthorized access to internal functionality or data. This issue is not exploitable from remote networks.	2025-09-11	8.7
CVE-2025-36222	ibm - multiple products	IBM Fusion 2.2.0 through 2.10.1, IBM Fusion HCI 2.2.0 through 2.10.0, and IBM Fusion HCI for watsonx 2.8.2 through 2.10.0 uses insecure default configurations that could expose AMQStreams without client authentication that could allow an attacker to perform unauthorized actions.	2025-09-11	8.7
CVE-2025-54256	adobe - dreamweaver	Dreamweaver Desktop versions 21.5 and earlier are affected by a Cross-Site Request Forgery (CSRF) 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 click on a malicious link, and scope is changed.	2025-09-09	8.6
CVE-2025-9201	lenovo - Browser	A potential DLL hijacking vulnerability was discovered in Lenovo Browser during an internal security assessment that could allow a local user to execute code with elevated privileges.	2025-09-11	8.5
CVE-2025-54910	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-09-09	8.4
CVE-2025-43884	dell - powerprotect_data_manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2025-09-10	8.2
CVE-2025-36854	microsoft - multiple products	A vulnerability (CVE-2024-38229 https://www.cve.org/CVERecord) exists in EOL ASP.NET when closing an HTTP/3 stream while application code is writing to the response body, a race condition may lead to use-after-free, resulting in Remote Code Execution. Per CWE-416: Use After Free https://cwe.mitre.org/data/definitions/416.html , Use After Free is when a product reuses or references memory after it has been freed. At some point afterward, the memory may be allocated again and saved in another pointer, while the original pointer references a location somewhere within the new allocation. Any operations using the original pointer are no longer valid because the memory "belongs" to the code that operates on the new pointer. This issue affects EOL ASP.NET 6.0.0 <= 6.0.36 as represented in this CVE, as well as 8.0.0 <= 8.0.8, 9.0.0-preview.1.24081.5 <= 9.0.0.RC.1 as represented in CVE-2024-38229 https://www.cve.org/CVERecord . Additionally, if you've deployed self-contained applications https://docs.microsoft.com/dotnet/core/deploying/#self-contained-deployments-scd targeting any of the impacted versions, these applications are also vulnerable and must be recompiled and redeployed.	2025-09-08	8.1

		NOTE: This CVE only represents End Of Life (EOL) software components. The vendor, Microsoft, has indicated there will be no future updates nor support provided upon inquiry.		
CVE-2025-49692	microsoft - Azure Connected Machine Agent	Improper access control in Azure Windows Virtual Machine Agent allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-53800	microsoft - multiple products	No cwe for this issue in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-53801	microsoft - multiple products	Untrusted pointer dereference in Windows DWM allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54091	microsoft - multiple products	Integer overflow or wraparound in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54092	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54098	microsoft - multiple products	Improper access control in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54102	microsoft - multiple products	Use after free in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54111	microsoft - multiple products	Use after free in Windows UI XAML Phone DatePickerFlyout allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54894	microsoft - multiple products	Local Security Authority Subsystem Service Elevation of Privilege Vulnerability	2025-09-09	7.8
CVE-2025-54895	microsoft - multiple products	Integer overflow or wraparound in Windows SPNEGO Extended Negotiation allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54896	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54898	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54899	microsoft - multiple products	Free of memory not on the heap in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54900	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54902	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54903	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54904	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54906	microsoft - multiple products	Free of memory not on the heap in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54907	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54908	microsoft - multiple products	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-54912	microsoft - multiple products	Use after free in Windows BitLocker allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54913	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows UI XAML Maps MapControlSettings allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54916	microsoft - multiple products	Stack-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-55224	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-55228	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2025-09-09	7.8
CVE-2025-55245	microsoft - xbox_gaming_services	Improper link resolution before file access ('link following') in Xbox allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-55316	microsoft - azure_connected_machine_agent	External control of file name or path in Azure Arc allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-55317	microsoft - autoupdate	Improper link resolution before file access ('link following') in Microsoft AutoUpdate (MAU) allows an authorized attacker to elevate privileges locally.	2025-09-09	7.8
CVE-2025-54242	adobe - multiple products	Premiere Pro versions 25.3, 24.6.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file, and scope is unchanged.	2025-09-09	7.8
CVE-2025-54257	adobe - multiple products	Acrobat Reader versions 24.001.30254, 20.005.30774, 25.001.20672 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file, and scope is unchanged.	2025-09-09	7.8
CVE-2025-54243	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.1 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.	2025-09-09	7.8
CVE-2025-54244	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.1 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.	2025-09-09	7.8
CVE-2025-54245	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.1 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.	2025-09-09	7.8

CVE-2025-54258	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	2025-09-09	7.8
CVE-2025-54259	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.2 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. Scope is unchanged.	2025-09-09	7.8
CVE-2025-54260	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is unchanged.	2025-09-09	7.8
CVE-2025-43725	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, Generic Application Agent, version(s) 19.19 and 19.20, contain(s) an Incorrect Default Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2025-09-10	7.8
CVE-2025-43885	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2025-09-10	7.8
CVE-2025-54248	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Scope is changed	2025-09-09	7.7
CVE-2025-55148	ivanti - multiple products	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	2025-09-09	7.6
CVE-2025-36853	microsoft - multiple products	A vulnerability (CVE-2025-21172) exists in msdia140.dll due to integer overflow and heap-based overflow. Per CWE-122: Heap-based Buffer Overflow, a heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). Per CWE-190: Integer Overflow or Wraparound, is when a product performs a calculation that can produce an integer overflow or wraparound when the logic assumes that the resulting value will always be larger than the original value. This occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may become a very small or negative number. 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.	2025-09-08	7.5
CVE-2025-53805	microsoft - multiple products	Out-of-bounds read in Windows Internet Information Services allows an unauthorized attacker to deny service over a network.	2025-09-09	7.5
CVE-2025-54919	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2025-09-09	7.5
CVE-2025-55243	microsoft - Microsoft OfficePLUS	Exposure of sensitive information to an unauthorized actor in Microsoft Office Plus allows an unauthorized attacker to perform spoofing over a network.	2025-09-09	7.5
CVE-2025-9319	lenovo - Wallpaper Client	A potential vulnerability was reported in the Lenovo Wallpaper Client that could allow arbitrary code execution under certain conditions.	2025-09-11	7.5
CVE-2025-27240	zabbix - Zabbix	A Zabbix adminitrator can inject arbitrary SQL during the autoremoval of hosts by inserting malicious SQL in the 'Visible name' field.	2025-09-12	7.5
CVE-2025-54103	microsoft - multiple products	Use after free in Windows Management Services allows an unauthorized attacker to elevate privileges locally.	2025-09-09	7.4
CVE-2025-20340	cisco - Cisco IOS XR Software	A vulnerability in the Address Resolution Protocol (ARP) implementation of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to trigger a broadcast storm, leading to a denial of service (DoS) condition on an affected device.&nbsp;_x000D_ _x000D_ This vulnerability is due to how Cisco IOS XR Software processes a high, sustained rate of ARP traffic hitting the management interface. Under certain conditions, an attacker could exploit this vulnerability by sending an excessive amount of traffic to the management interface of an affected device, overwhelming its ARP processing capabilities. A successful exploit could result in degraded device performance, loss of management connectivity, and complete unresponsiveness of the system, leading to a DoS condition.	2025-09-10	7.4
CVE-2025-43790	liferay - multiple products	Insecure Direct Object Reference (IDOR) vulnerability in Liferay Portal 7.4.0 through 7.4.3.124, and Liferay DXP 2024.Q2.0 through 2024.Q2.6, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows remote authenticated users to from one virtual instance to access, create, edit, relate data/object entries/definitions to an object in a different virtual instance.	2025-09-11	7.4
CVE-2025-54116	microsoft - multiple products	Improper access control in Windows MultiPoint Services allows an authorized attacker to elevate privileges locally.	2025-09-09	7.3
CVE-2025-54911	microsoft - multiple products	Use after free in Windows BitLocker allows an authorized attacker to elevate privileges locally.	2025-09-09	7.3
CVE-2025-55236	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Graphics Kernel allows an authorized attacker to execute code locally.	2025-09-09	7.3
CVE-2025-8061	lenovo - multiple products	A potential insufficient access control vulnerability was reported in the Lenovo Dispatcher 3.0 and Dispatcher 3.1 drivers used by some Lenovo consumer notebooks that could allow an authenticated local user to execute code with elevated privileges. The Lenovo Dispatcher 3.2 driver is not affected. This vulnerability does not affect systems when the Windows feature Core Isolation Memory	2025-09-11	7.3

		Integrity is enabled. Lenovo systems preloaded with Windows 11 have this feature enabled by default.		
CVE-2025-27234	zabbix - Zabbix	Zabbix Agent 2 smartctl plugin does not properly sanitize smart.disk.get parameters, allowing an attacker to inject unexpected arguments into the smartctl command. In Zabbix 5.0 this allows for remote code execution.	2025-09-12	7.3
CVE-2025-54905	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2025-09-09	7.1
CVE-2025-43796	liferay - multiple products	Liferay Portal 7.4.0 through 7.4.3.101, and Liferay DXP 2023.Q3.0 through 2023.Q3.4, 7.4 GA through update 92 and 7.3 GA though update 35 does not limit the number of objects returned from a GraphQL queries, which allows remote attackers to perform denial-of-service (DoS) attacks on the application by executing queries that return a large number of objects.	2025-09-12	7.1
CVE-2025-49734	microsoft - multiple products	Improper restriction of communication channel to intended endpoints in Windows PowerShell allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-53802	microsoft - multiple products	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-53807	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-54093	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-54099	microsoft - multiple products	Stack-based buffer overflow in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-54105	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-54108	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Capability Access Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-54112	microsoft - multiple products	Use after free in Microsoft Virtual Hard Drive allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-54114	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Connected Devices Platform Service allows an authorized attacker to deny service locally.	2025-09-09	7.0
CVE-2025-54115	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-55223	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to elevate privileges locally.	2025-09-09	7.0
CVE-2025-43887	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) an Incorrect Default Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2025-09-10	7.0
CVE-2025-40594	siemens - multiple products	A vulnerability has been identified in SINAMICS G220 V6.4 (All versions < V6.4 HF2), SINAMICS S200 V6.4 (All versions), SINAMICS S210 V6.4 (All versions < V6.4 HF2). The affected devices allow a factory reset to be executed without the required privileges due to improper privilege management as well as manipulation of configuration data because of leaked privileges of previous sessions. This could allow an unauthorized attacker to escalate their privileges.	2025-09-09	6.9
CVE-2025-43786	liferay - multiple products	Enumeration of ERC from object entry in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.1, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12, 2023.Q4.0 and 7.4 GA through update 92 allow attackers to determine existent ERC in the application by exploit the time response.	2025-09-09	6.9
CVE-2025-55139	ivanti - multiple products	SSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to enumerate internal services.	2025-09-09	6.8
CVE-2025-43722	dell - multiple products	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper privilege management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2025-09-08	6.7
CVE-2024-45325	fortinet - fortiddos-f	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiDDoS-F version 7.0.0 through 7.02 and before 6.6.3 may allow a privileged attacker to execute unauthorized code or commands via crafted CLI requests.	2025-09-09	6.7
CVE-2025-53808	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7
CVE-2025-53810	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7
CVE-2025-54094	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7
CVE-2025-54104	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7
CVE-2025-54109	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7
CVE-2025-54915	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Defender Firewall Service allows an authorized attacker to elevate privileges locally.	2025-09-09	6.7
CVE-2025-55226	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Graphics Kernel allows an authorized attacker to execute code locally.	2025-09-09	6.7
CVE-2025-58782	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Jackrabbit Core and Apache Jackrabbit JCR Commons. This issue affects Apache Jackrabbit Core: from 1.0.0 through 2.22.1; Apache Jackrabbit JCR Commons: from 1.0.0 through 2.22.1. Deployments that accept JNDI URIs for JCR lookup from untrusted users allows them to inject malicious JNDI references, potentially leading to arbitrary code execution through deserialization of untrusted data.	2025-09-08	6.5

		Users are recommended to upgrade to version 2.22.2. JCR lookup through JNDI has been disabled by default in 2.22.2. Users of this feature need to enable it explicitly and are adviced to review their use of JNDI URI for JCR lookup.		
CVE-2025-47997	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in SQL Server allows an authorized attacker to disclose information over a network.	2025-09-09	6.5
CVE-2025-53796	microsoft - multiple products	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5
CVE-2025-53797	microsoft - multiple products	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5
CVE-2025-53798	microsoft - multiple products	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5
CVE-2025-53806	microsoft - multiple products	Buffer over-read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network.	2025-09-09	6.5
CVE-2025-53809	microsoft - multiple products	Improper input validation in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.	2025-09-09	6.5
CVE-2025-54095	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.	2025-09-09	6.5
CVE-2025-54096	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.	2025-09-09	6.5
CVE-2025-54097	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.	2025-09-09	6.5
CVE-2025-54246	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 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 write access.	2025-09-09	6.5
CVE-2025-54247	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access.	2025-09-09	6.5
CVE-2025-54249	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to manipulate server-side requests and bypass security controls allowing unauthorized read access.	2025-09-09	6.5
CVE-2025-55225	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.	2025-09-09	6.5
CVE-2024-45669	ibm - security_verify_information_queue	IBM Security Verify Information Queue 10.0.5, 10.0.6, 10.0.7, and 10.0.8 could allow a remote user to cause a denial of service due to improper handling of special characters that could lead to uncontrolled resource consumption.	2025-09-10	6.5
CVE-2025-36125	ibm - Hardware Management Console	IBM Hardware Management Console - Power 10.3.1050.0 and 11.1.1110.0 is vulnerable to stored 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.	2025-09-09	6.4
CVE-2024-47120	ibm - security_verify_information_queue	IBM Security Verify Information Queue 10.0.5, 10.0.6, 10.0.7, and 10.0.8 could allow a privileged user to escalate their privileges and attack surface on the host due to the containers running with unnecessary privileges.	2025-09-10	6.4
CVE-2025-40757	siemens - multiple products	A vulnerability has been identified in APOGEE PXC Series (BACnet) (All versions), APOGEE PXC Series (P2 Ethernet) (All versions), TALON TC Series (BACnet) (All versions). Affected devices connected to the network allow unrestricted access to sensitive files, such as databases. This could allow an attacker to download encrypted .db file containing passwords.	2025-09-09	6.3
CVE-2025-43784	liferay - multiple products	Improper Access Control vulnerability in Liferay Portal 7.4.0 through 7.4.3.124, and Liferay DXP 2024.Q2.0 through 2024.Q2.8, 2024.Q1.1 through 2024.Q1.12 and 7.4 GA through update 92 allows guest users to obtain object entries information via the API Builder.	2025-09-10	6.2
CVE-2025-55143	ivanti - multiple products	Reflected text injection in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to inject arbitrary text into a crafted HTTP response. User interaction is required.	2025-09-09	6.1
CVE-2025-20248	cisco - Cisco IOS XR Software	A vulnerability in the installation process of Cisco IOS XR Software could allow an authenticated, local attacker to bypass Cisco IOS XR Software image signature verification and load unsigned software on an affected device. To exploit this vulnerability, the attacker must have root-system privileges on the affected device. This vulnerability is due to incomplete validation of files during the installation of an .iso file. An attacker could exploit this vulnerability by modifying contents of the .iso image and then installing and activating it on the device. A successful exploit could allow the attacker to load an unsigned file as part of the image activation process.	2025-09-10	6.0
CVE-2025-1761	ibm - concert	IBM Concert Software 1.0.0 through 1.1.0 could allow a remote attacker to obtain sensitive information from allocated memory due to improper clearing of heap memory.	2025-09-08	5.9
CVE-2024-45671	ibm - security_verify_information_queue	IBM Security Verify Information Queue 10.0.5, 10.0.6, 10.0.7, and 10.0.8 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2025-09-10	5.9
CVE-2025-27233	zabbix - Zabbix	Zabbix Agent 2 smartctl plugin does not properly sanitize smart.disk.get parameters, allowing an attacker to inject unexpected arguments into the smartctl command. This can be used to leak the NTLMv2 hash from a Windows system.	2025-09-12	5.7
CVE-2025-10093	d-link - DIR-852	A vulnerability was identified in D-Link DIR-852 up to 1.00CN B09. Affected by this vulnerability is the function phpcgi_main of the file /getcfg.php of the component Device Configuration Handler. Such manipulation leads to information disclosure. The attack may be performed from remote. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-08	5.5
CVE-2025-53799	microsoft - multiple products	Use of uninitialized resource in Windows Imaging Component allows an unauthorized attacker to disclose information locally.	2025-09-09	5.5

CVE-2025-53803	microsoft - multiple products	Generation of error message containing sensitive information in Windows Kernel allows an authorized attacker to disclose information locally.	2025-09-09	5.5
CVE-2025-53804	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2025-09-09	5.5
CVE-2025-54901	microsoft - multiple products	Buffer over-read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2025-09-09	5.5
CVE-2025-54239	adobe - multiple products	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	5.5
CVE-2025-54240	adobe - multiple products	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	5.5
CVE-2025-54241	adobe - multiple products	After Effects versions 25.3, 24.6.7 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure, potentially disclosing sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-09	5.5
CVE-2025-55144	ivanti - multiple products	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	2025-09-09	5.4
CVE-2025-8711	ivanti - multiple products	CSRF in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote unauthenticated attacker to execute limited actions on behalf of the victim user. User interaction is required.	2025-09-09	5.4
CVE-2025-8712	ivanti - multiple products	Missing authorization in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 22.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with read-only admin privileges to configure restricted settings.	2025-09-09	5.4
CVE-2025-54252	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 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. This could result in bypassing security features within the application. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field.	2025-09-09	5.4
CVE-2025-43781	liferay - multiple products	Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.110 through 7.4.3.128, and Liferay DXP 2024.Q3.1 through 2024.Q3.8, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.12 allows remote attackers to inject arbitrary web script or HTML via the URL in search bar portlet	2025-09-09	5.3
CVE-2025-20159	cisco - Cisco IOS XR Software	A vulnerability in the management interface access control list (ACL) processing feature in Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass configured ACLs for the SSH, NetConf, and gRPC features. This vulnerability exists because management interface ACLs have not been supported on Cisco IOS XR Software Packet I/O infrastructure platforms for Linux-handled features such as SSH, NetConf, or gRPC. An attacker could exploit this vulnerability by attempting to send traffic to an affected device. A successful exploit could allow the attacker to bypass an ingress ACL that is applied on the management interface of the affected device.	2025-09-10	5.3
CVE-2025-43782	liferay - multiple products	Insecure Direct Object Reference (IDOR) vulnerability in Liferay Portal 7.4.0 through 7.4.3.124, and Liferay DXP 2024.Q2.0 through 2024.Q2.7, 2024.Q1.1 through 2024.Q1.12, and 7.4 GA through update 92 allows remote authenticated users to access a workflow definition by name via the API	2025-09-11	5.3
CVE-2025-9214	lenovo - multiple products	A missing authentication vulnerability was reported in some Lenovo printers that could allow a user to view limited device information or modify network settings via the CUPS service.	2025-09-11	5.3
CVE-2025-43788	liferay - multiple products	The organization selector in Liferay Portal 7.4.0 through 7.4.3.124, and Liferay DXP 2024.Q1.1 through 2024.Q1.12 and 7.4 update 81 through update 85 does not check user permission, which allows remote authenticated users to obtain a list of all organizations.	2025-09-12	5.3
CVE-2025-36100	ibm - MQ	IBM MQ LTS 9.1.0.0 through 9.1.0.29, 9.2.0.0 through 9.2.0.36, 9.3.0.0 through 9.3.0.30 and 9.4.0.0 through 9.4.0.12 and IBM MQ CD 9.3.0.0 through 9.3.5.1 and 9.4.0.0 through 9.4.3.0 Java and JMS stores a password in client configuration files when trace is enabled which can be read by a local user.	2025-09-07	5.1
CVE-2025-43777	liferay - multiple products	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.19 exposes "Internal Server Error" in the response body when a login attempt is made with a deleted Client Secret.	2025-09-09	5.1
CVE-2025-10107	trendnet - TEW-831DR	A vulnerability has been found in TRENDnet TEW-831DR 1.0 (601.130.1.1410). Impacted is an unknown function of the file /boafrm/formSysCmd. The manipulation of the argument sysHost leads to command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-09-09	5.1
CVE-2025-43783	liferay - multiple products	Reflected cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.73 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.1, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.12, 7.4 update 73 through update 92 allows remote attackers to inject arbitrary web script or HTML via the /c/portal/comment/discussion/get_editor path.	2025-09-10	5.1
CVE-2025-43787	liferay - multiple products	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q3.0, 2025.Q2.0 through 2025.Q2.12, 2025.Q1.0 through 2025.Q1.17, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 allows an remote authenticated attacker to inject JavaScript through the organization site names. The malicious payload is stored and executed without proper sanitization or escaping.	2025-09-12	5.1
CVE-2025-43795	liferay - multiple products	Open redirect vulnerability in the System Settings in Liferay Portal 7.1.0 through 7.4.3.101, and Liferay DXP 2023.Q3.1 through 2023.Q3.4 , 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_configuration_admin_web_portlet_SystemSettingsPortlet_redirect parameter.	2025-09-12	5.1

		Open redirect vulnerability in the Instance Settings in Liferay Portal 7.1.0 through 7.4.3.101, and Liferay DXP 2023.Q3.1 through 2023.Q3.4 , 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_configuration_admin_web_portlet_InstanceSettingsPortlet_redirect parameter. Open redirect vulnerability in the Site Settings in Liferay Portal 7.1.0 through 7.4.3.101, and Liferay DXP 2023.Q3.1 through 2023.Q3.4 , 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to redirect users to arbitrary external URLs via the _com_liferay_site_admin_web_portlet_SiteSettingsPortlet_redirect parameter.		
CVE-2025-43938	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) a Plaintext Storage of a Password vulnerability. A high privileged attacker with local 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 gain unauthorized access with privileges of the compromised account.	2025-09-10	5.0
CVE-2025-53609	fortinet - multiple products	A Relative Path Traversal vulnerability [CWE-23] in FortiWeb 7.6.0 through 7.6.4, 7.4.0 through 7.4.8, 7.2.0 through 7.2.11, 7.0.2 through 7.0.11 may allow an authenticated attacker to perform an arbitrary file read on the underlying system via crafted requests.	2025-09-09	4.9
CVE-2025-55146	ivanti - multiple products	An unchecked return value in Ivanti Connect Secure before 22.7R2.9 or 22.8R2, Ivanti Policy Secure before 22.7R1.6, Ivanti ZTA Gateway before 2.8R2.3-723 and Ivanti Neurons for Secure Access before 22.8R1.4 (Fix deployed on 02-Aug-2025) allows a remote authenticated attacker with admin privileges to trigger a denial of service.	2025-09-09	4.9
CVE-2025-54250	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access.	2025-09-09	4.9
CVE-2025-43763	liferay - multiple products	A server-side request forgery (SSRF) vulnerability exist in the Liferay Portal 7.4.0 through 7.4.3.131, and Liferay DXP 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 that affects custom object attachment fields. This flaw allows an attacker to manipulate the application into making unauthorized requests to other instances, creating new object entries that link to external resources.	2025-09-09	4.8
CVE-2025-43778	liferay - multiple products	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.11, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13 and 2024.Q1.1 through 2024.Q1.20 allows an remote authenticated attacker to inject JavaScript through the name of a fieldset in Kaleo Forms Admin. The malicious payload is stored and executed without proper sanitization or escaping.	2025-09-09	4.8
CVE-2025-54101	microsoft - multiple products	Use after free in Windows SMBv3 Client allows an authorized attacker to execute code over a network.	2025-09-09	4.8
CVE-2025-43776	liferay - multiple products	A Stored cross-site scripting vulnerability in the Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q2.0 through 2025.Q2.9, 2025.Q1.0 through 2025.Q1.16, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.0 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.19 and 7.4 GA through update 92 allows an remote authenticated attacker to inject JavaScript through Custom Object field label. The malicious payload is stored and executed through Process Builder's Configuration tab without proper escaping.	2025-09-09	4.6
CVE-2025-43775	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.128, and Liferay DXP 2024.Q3.0 through 2024.Q3.5, 2024.Q2.0 through 2024.Q2.12, 2024.Q1.1 through 2024.Q1.12, and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via remote app title field.	2025-09-09	4.6
CVE-2025-43785	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.3.45 through 7.4.3.128, and Liferay DXP 2024 Q2.0 through 2024.Q2.9, 2024.Q1.1 through 2024.Q1.12, and 7.4 update 45 through update 92 allows remote attackers to execute an arbitrary web script or HTML in the My Workflow Tasks page.	2025-09-10	4.6
CVE-2025-43886	dell - PowerProtect Data Manager	Dell PowerProtect Data Manager, version(s) 19.19 and 19.20, Hyper-V contain(s) a Path Traversal: '.../...//' vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2025-09-10	4.4
CVE-2025-54107	microsoft - multiple products	Improper resolution of path equivalence in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	2025-09-09	4.3
CVE-2025-54251	adobe - multiple products	Adobe Experience Manager versions 6.5.23.0 and earlier are affected by an XML Injection vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to manipulate XML queries and gain limited unauthorized write access.	2025-09-09	4.3
CVE-2025-54917	microsoft - multiple products	Protection mechanism failure in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	2025-09-09	4.3
CVE-2025-36011	ibm - Jazz for Service Management	IBM Jazz for Service Management 1.1.3.0 through 1.1.3.24 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	2025-09-09	4.3
CVE-2025-54255	adobe - multiple products	Acrobat Reader versions 24.001.30254, 20.005.30774, 25.001.20672 and earlier are affected by a Violation of Secure Design Principles vulnerability that could result in a security feature bypass. Exploitation of this issue does not require user interaction, and scope is unchanged.	2025-09-09	4.0
CVE-2025-8277	red hat - multiple products	A flaw was found in libssh's handling of key exchange (KEX) processes when a client repeatedly sends incorrect KEX guesses. The library fails to free memory during these rekey operations, which can gradually exhaust system memory. This issue can lead to crashes on the client side, particularly when using libgcrypt, which impacts application stability and availability.	2025-09-09	3.1
CVE-2025-40802	siemens - RUGGEDCOM RST2428P	A vulnerability has been identified in RUGGEDCOM RST2428P (6GK6242-6PA00) (All versions). The affected device may be susceptible to resource exhaustion when subjected to high volumes of query requests._x000D_ This could allow an attacker to cause a temporary denial of service, with the system recovering once the activity stops.	2025-09-09	2.3

CVE-2025-40803	siemens - RUGGEDCOM RST2428P	A vulnerability has been identified in RUGGEDCOM RST2428P (6GK6242-6PA00) (All versions). The affected device exposes certain non-critical information from the device. This could allow an unauthenticated attacker to access sensitive data, potentially leading to a breach of confidentiality.	2025-09-09	2.3
CVE-2025-27238	zabbix - Zabbix	Due to a bug in Zabbix API, the hostprototype.get method lists all host prototypes to users that do not have any user groups assigned to them.	2025-09-12	2.1
CVE-2025-43789	liferay - multiple products	JSON Web Services in Liferay Portal 7.4.0 through 7.4.3.119, and Liferay DXP 2024.Q1.1 through 2024.Q1.9, 7.4 GA through update 92 published to OSGi are registered and invoked directly as classes which allows Service Access Policies get executed.	2025-09-12	1.0

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.