الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ١٢ أكتوبر إلى ١٨ أكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 12th of October to 18th of October. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-49708	microsoft - multiple products	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges over a network.	2025-10-14	9.9
CVE-2025-55315	microsoft - multiple products	Inconsistent interpretation of http requests ('http request/response smuggling') in ASP.NET Core allows an authorized attacker to bypass a security feature over a network.	2025-10-14	9.9
CVE-2025-11708	mozilla - multiple products	Use-after-free in MediaTrackGraphImpl::GetInstance() This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	9.8
CVE-2025-11709	mozilla - multiple products	A compromised web process was able to trigger out of bounds reads and writes in a more privileged process using manipulated WebGL textures. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	9.8
CVE-2025-11710	mozilla - multiple products	A compromised web process using malicious IPC messages could have caused the privileged browser process to reveal blocks of its memory to the compromised process. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	9.8
CVE-2025-11719	mozilla - multiple products	Starting in Firefox 143, the use of the native messaging API by web extensions on Windows could lead to crashes caused by use-after-free memory corruption. This vulnerability affects Firefox < 144 and Thunderbird < 144.	2025-10-14	9.8
CVE-2025-11721	mozilla - multiple products	Memory safety bug present in Firefox 143 and Thunderbird 143. This bug showed evidence of memory corruption and we presume that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144 and Thunderbird < 144.	2025-10-14	9.8
CVE-2025-59287	microsoft - multiple products	Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.	2025-10-14	9.8
CVE-2025-54539	apache - activemq_nms_amqp	A Deserialization of Untrusted Data vulnerability exists in the Apache ActiveMQ NMS AMQP Client. This issue affects all versions of Apache ActiveMQ NMS AMQP up to and including 2.3.0, when establishing connections to untrusted AMQP servers. Malicious servers could exploit unbounded deserialization logic present in the client to craft responses that may lead to arbitrary code execution on the client side. Although version 2.1.0 introduced a mechanism to restrict deserialization via allow/deny lists, the protection was found to be bypassable under certain conditions. In line with Microsoft's deprecation of binary serialization in .NET 9, the project is evaluating the removal of .NET binary serialization support from the NMS API entirely in future releases. Mitigation and Recommendations: Users are strongly encouraged to upgrade to version 2.4.0 or later, which resolves the issue. Additionally, projects depending on NMS-AMQP should migrate away from .NET binary serialization as part of a long-term hardening strategy.	2025-10-16	9.8
CVE-2025-10611	wso2 - multiple products	Due to an insufficient access control implementation in multiple WSO2 Products, authentication and authorization checks for certain REST APIs can be bypassed, allowing them to be invoked without proper validation. Successful exploitation of this vulnerability could lead to a malicious actor gaining administrative access and performing unauthenticated and unauthorized administrative operations.	2025-10-16	9.8
CVE-2025-9152	wso2 - multiple products	An improper privilege management vulnerability exists in WSO2 API Manager due to missing authentication and authorization checks in the keymanager-operations Dynamic Client Registration (DCR) endpoint.	2025-10-16	9.8

		A malicious user can exploit this flaw to generate access tokens with elevated privileges, potentially leading to administrative access and the ability to perform unauthorized operations.		
CVE-2023-28814	hikvision - iSecure Center	Some versions of Hikvision's iSecure Center Product have an improper file upload control vulnerability. Due to the improper verification of file to be uploaded, attackers may upload malicious files to the server. iSecure Center is software released for China's domestic market only, with no overseas release.	2025-10-17	9.8
CVE-2023-28815	hikvision - iSecure Center	Some versions of Hikvision's iSecure Center Product contain insufficient parameter validation, resulting in a command injection vulnerability. Attackers may exploit this to gain platform privileges and execute arbitrary commands on the system.iSecure Center is software released for China's domestic market only, with no overseas release.	2025-10-17	9.8
CVE-2025-9804	wso2 - multiple products	An improper access control vulnerability exists in multiple WSO2 products due to insufficient permission enforcement in certain internal SOAP Admin Services and System REST APIs. A low-privileged user may exploit this flaw to perform unauthorized operations, including accessing server-level information. This vulnerability affects only internal administrative interfaces. APIs exposed through the WSO2 API Manager's API Gateway remain unaffected.	2025-10-16	9.6
CVE-2025-40765	siemens - telecontrol_server_basic	A vulnerability has been identified in TeleControl Server Basic V3.1 (All versions >= V3.1.2.2 < V3.1.2.3). The affected application contains an information disclosure vulnerability. This could allow an unauthenticated remote attacker to obtain password hashes of users and to login to and perform authenticated operations of the database service.	2025-10-14	9.3
CVE-2025-40771	siemens - multiple products	A vulnerability has been identified in SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0) (All versions < V2.4.24), SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0) (All versions < V2.4.24), SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0) (All versions < V2.4.24), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0) (All versions < V2.4.24). Affected devices do not properly authenticate configuration connections. This could allow an unauthenticated remote attacker to access the configuration data.	2025-10-14	9.3
CVE-2025-49553	adobe - connect	Adobe Connect versions 12.9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute malicious scripts in a victim's browser. Exploitation of this issue requires user interaction in that a victim must navigate to a crafted web page. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Scope is changed.	2025-10-14	9.3
CVE-2025-11717	mozilla - firefox	When switching between Android apps using the card carousel Firefox shows a black screen as its card image when a password-related screen was the last one being used. Prior to Firefox 144 the password edit screen was visible. This vulnerability affects Firefox < 144.	2025-10-14	9.1
CVE-2025-9713	ivanti - multiple products	Path traversal in Ivanti Endpoint Manager allows a remote unauthenticated attacker to achieve remote code execution. User interaction is required.	2025-10-13	8.8
CVE-2025-11714	mozilla - multiple products	Memory safety bugs present in Firefox ESR 115.28, Firefox ESR 140.3, Thunderbird ESR 140.3, Firefox 143 and Thunderbird 143. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	8.8
CVE-2025-11715	mozilla - multiple products	Memory safety bugs present in Firefox ESR 140.3, Thunderbird ESR 140.3, Firefox 143 and Thunderbird 143. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	8.8
CVE-2025-58715	microsoft - multiple products	Integer overflow or wraparound in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	2025-10-14	8.8
CVE-2025-58716	microsoft - multiple products	Improper input validation in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	2025-10-14	8.8
CVE-2025-58718	microsoft - multiple products	Use after free in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2025-10-14	8.8
CVE-2025-59228	microsoft - multiple products	Improper input validation in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-10-14	8.8
CVE-2025-59237	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2025-10-14	8.8
CVE-2025-59249	microsoft - multiple products	Weak authentication in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	2025-10-14	8.8
CVE-2025-59295	microsoft - multiple products	Heap-based buffer overflow in Internet Explorer allows an unauthorized attacker to execute code over a network.	2025-10-14	8.8
CVE-2025-47410	apache - geode	Apache Geode is vulnerable to CSRF attacks through GET requests to the Management and Monitoring REST API that could allow an attacker who has tricked a user into giving up their Geode session credentials to submit malicious commands on the target system on behalf of the authenticated user. This issue affects Apache Geode: versions 1.10 through 1.15.1 Users are recommended to upgrade to version 1.15.2, which fixes the issue.	2025-10-18	8.8
CVE-2011-20001	siemens - multiple products	A vulnerability has been identified in SIMATIC S7-1200 CPU V1 family (incl. SIPLUS variants) (All versions < V2.0.3), SIMATIC S7-1200 CPU V2 family (incl. SIPLUS variants) (All versions < V2.0.3). The web server interface of affected devices improperly processes incoming malformed HTTP traffic at high rate. This could allow an unauthenticated remote attacker to force the device entering the stop/defect state, thus creating a denial of service condition.	2025-10-14	8.7
CVE-2025-40755	siemens - multiple products	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP1). Affected applications are vulnerable to SQL injection through getTotalAndFilterCounts endpoint. An authenticated low privileged attacker could exploit to insert data and achieve privilege escalation. (ZDI-CAN-26570)	2025-10-14	8.7
CVE-2025-41430	f5 - multiple products	When BIG-IP SSL Orchestrator is enabled, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-46706	f5 - multiple products	When an iRule containing the HTTP::respond command is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7

CVE-2025-48008	f5 - multiple products	When a TCP profile with Multipath TCP (MPTCP) enabled is configured on a virtual server, undisclosed traffic along with conditions beyond the attacker's control can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-53474	f5 - multiple products	When an iRule using an ILX::call command is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-53521	f5 - multiple products	When a BIG-IP APM Access Policy is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-53856	f5 - multiple products	When a virtual server, network address translation (NAT) object, or secure network address translation (SNAT) object uses the embedded Packet Velocity Acceleration (ePVA) feature, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. To determine which BIG-IP platforms have an ePVA chip refer to K12837: Overview of the ePVA feature https://my.f5.com/manage/s/article/K12837 . Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-54479	f5 - multiple products	When a classification profile is configured on a virtual server without an HTTP or HTTP/2 profile, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-54854	f5 - multiple products	When a BIG-IP APM OAuth access profile (Resource Server or Resource Client) is configured on a virtual server, undisclosed traffic can cause the apmd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-54858	f5 - multiple products	When a BIG-IP Advanced WAF or BIG-IP ASM Security Policy is configured with a JSON content profile that has a malformed JSON schema, and the security policy is applied to a virtual server, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-55036	f5 - multiple products	When BIG-IP SSL Orchestrator explicit forward proxy is configured on a virtual server and the proxy connect feature is enabled, undisclosed traffic may cause memory corruption. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-55669	f5 - multiple products	When the BIG-IP Advanced WAF and ASM security policy and a server-side HTTP/2 profile are configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-58120	f5 - multiple products	When HTTP/2 Ingress is configured, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-59478	f5 - multiple products	When a BIG-IP AFM denial-of-service (DoS) protection profile is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-59781	f5 - multiple products	When DNS cache is configured on a BIG-IP or BIG-IP Next CNF virtual server, undisclosed DNS queries can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-60016	f5 - multiple products	When Diffie-Hellman (DH) group Elliptic Curve Cryptography (ECC) Brainpool curves are configured in an SSL profile's Cipher Rule or Cipher Group, and that profile is applied to a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-61938	f5 - multiple products	When a BIG-IP Advanced WAF or ASM security policy is configured with a URL greater than 1024 characters in length for the Data Guard Protection Enforcement setting, either manually or through the automatic Policy Builder, the bd process can terminate repeatedly. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-61951	f5 - multiple products	Undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. This issue may occur when a Datagram Transport Layer Security (DTLS) 1.2 virtual server is enabled with a Server SSL profile that is configured with a certificate, key, and the SSL Sign Hash set to ANY, and the backend server is enabled with DTLS 1.2 and client authentication. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-61960	f5 - multiple products	When a per-request policy is configured on a BIG-IP APM portal access virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-61974	f5 - multiple products	When a client SSL profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-58071	f5 - multiple products	When IPsec is configured on the BIG-IP system, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-61935	f5 - multiple products	When a BIG IP Advanced WAF or ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-61990	f5 - multiple products	When using a multi-bladed platform with more than one blade, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.7
CVE-2025-53868	f5 - multiple products	When running in Appliance mode, a highly privileged authenticated attacker with access to SCP and SFTP may be able to bypass Appliance mode restrictions using undisclosed commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.5
CVE-2025-59481	f5 - multiple products	A vulnerability exists in an undisclosed iControl REST and BIG-IP TMOS Shell (tmsh) command that may allow an authenticated attacker with at least resource administrator role to execute arbitrary system commands with higher privileges. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.5

CVE-2025-59483	f5 - multiple products	A validation vulnerability exists in an undisclosed URL in the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.5
CVE-2025-61955	f5 - multiple products	A vulnerability exists in F5OS-A and F5OS-C systems that may allow an authenticated attacker with local access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.5
CVE-2025-61958	f5 - multiple products	A vulnerability exists in the iHealth command that may allow an authenticated attacker with at least a resource administrator role to bypass tmsh restrictions and gain access to a bash shell. For BIG-IP systems running in Appliance mode, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.5
CVE-2025-10581	lenovo - PC Manager	A potential DLL hijacking vulnerability was discovered in the Lenovo PC Manager during an internal security assessment that could allow a local authenticated user to execute code with elevated privileges.	2025-10-15	8.5
CVE-2025-8486	lenovo - PC Manager	A potential vulnerability was reported in PC Manager that could allow a local authenticated user to execute code with elevated privileges.	2025-10-15	8.5
CVE-2025-57780	f5 - multiple products	A vulnerability exists in F5OS-A and F5OS-C system that may allow an authenticated attacker with local access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.5
CVE-2025-53782	microsoft - multiple products	Incorrect implementation of authentication algorithm in Microsoft Exchange Server allows an unauthorized attacker to elevate privileges locally.	2025-10-14	8.4
CVE-2025-59213	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Configuration Manager allows an unauthorized attacker to elevate privileges locally.	2025-10-14	8.4
CVE-2025-59236	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	8.4
CVE-2025-59269	f5 - multiple products	A stored cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.4
CVE-2025-43281	apple - macos	The issue was addressed with improved authentication. This issue is fixed in macOS Sequoia 15.6. A local attacker may be able to elevate their privileges.	2025-10-15	8.4
CVE-2011-20002	siemens - multiple products	A vulnerability has been identified in SIMATIC S7-1200 CPU V1 family (incl. SIPLUS variants) (All versions < V2.0.2), SIMATIC S7-1200 CPU V2 family (incl. SIPLUS variants) (All versions < V2.0.2). Affected controllers are vulnerable to capture-replay in the communication with the engineering software. This could allow an on-path attacker between the engineering software and the controller to execute any previously recorded commands at a later time (e.g. set the controller to STOP), regardless whether or not the controller had a password configured.	2025-10-14	8.3
CVE-2025-58325	fortinet - multiple products	An Incorrect Provision of Specified Functionality vulnerability [CWE-684] in FortiOS 7.6.0, 7.4.0 through 7.4.5, 7.2.5 through 7.2.10, 7.0.0 through 7.0.15, 6.4 all versions may allow a local authenticated attacker to execute system commands via crafted CLI commands.	2025-10-14	8.2
CVE-2025-59291	microsoft - azure_compute_gallery	External control of file name or path in Confidential Azure Container Instances allows an authorized attacker to elevate privileges locally.	2025-10-14	8.2
CVE-2025-59292	microsoft - azure_compute_gallery	External control of file name or path in Confidential Azure Container Instances allows an authorized attacker to elevate privileges locally.	2025-10-14	8.2
CVE-2025-58096	f5 - multiple products	When the database variable tm.tcpudptxchecksum is configured as non-default value Software-only on a BIG-IP system, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.2
CVE-2025-58153	f5 - multiple products	Under undisclosed traffic conditions along with conditions beyond the attacker's control, hardware systems with a High-Speed Bridge (HSB) may experience a lockup of the HSB. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	8.2
CVE-2025-36087	ibm - multiple products	IBM Security Verify Access 10.0.0 through 10.0.9, 11.0.0, IBM Verify Identity Access Container 10.0.0 through 10.0.9, and 11.0.0, under certain configurations, contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2025-10-13	8.1
CVE-2025-11713	mozilla - multiple products	Insufficient escaping in the “Copy as cURL” feature could have been used to trick a user into executing unexpected code on Windows. This did not affect Firefox running on other operating systems. This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	8.1
CVE-2025-11720	mozilla - firefox	The Firefox and Firefox Focus UI for the Android custom tab feature only showed the "site" that was loaded, not the full hostname. User supplied content hosted on a subdomain of a site could have been used to fool a user into thinking it was content from a different subdomain of that site. This vulnerability affects Firefox < 144.	2025-10-14	8.1
CVE-2025-49201	fortinet - multiple products	A weak authentication in Fortinet FortiPAM 1.5.0, 1.4.0 through 1.4.2, 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager 7.2.0 through 7.2.4 allows attacker to execute unauthorized code or commands via specially crafted http requests	2025-10-14	8.1
CVE-2025-59250	microsoft - multiple products	Improper input validation in JDBC Driver for SQL Server allows an unauthorized attacker to perform spoofing over a network.	2025-10-14	8.1
CVE-2025-54263	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 Incorrect Authorization vulnerability. A low-privileged attacker could leverage this vulnerability to bypass security measures and maintain unauthorized access. Exploitation of this issue does not require user interaction.	2025-10-14	8.1

CVE-2025-54264	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 a stored Cross-Site Scripting (XSS) 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. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field. Scope is changed.	2025-10-14	8.1
CVE-2025-11695	mongodb - Rust Driver	When tlsInsecure=False appears in a connection string, certificate validation is disabled. This vulnerability affects MongoDB Rust Driver versions prior to v3.2.5	2025-10-13	8.0
CVE-2025-11622	ivanti - multiple products	Insecure deserialization in Ivanti Endpoint Manager allows a local authenticated attacker to escalate their privileges.	2025-10-13	7.8
CVE-2025-20723	google - multiple products	In gnss driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09920033; Issue ID: MSV-3797.	2025-10-14	7.8
CVE-2025-57741	fortinet - multiple products	An Incorrect Permission Assignment for Critical Resource vulnerability [CWE-732] in FortiClientMac 7.4.0 through 7.4.3, 7.2.0 through 7.2.11, 7.0 all versions may allow a local attacker to run arbitrary code or commands via LaunchDaemon hijacking.	2025-10-14	7.8
CVE-2025-24052	microsoft - multiple products	Microsoft is aware of vulnerabilities in the third party Agere Modem driver that ships natively with supported Windows operating systems. This is an announcement of the upcoming removal of ltmdm64.sys driver. The driver has been removed in the October cumulative update. Fax modem hardware dependent on this specific driver will no longer work on Windows. Microsoft recommends removing any existing dependencies on this hardware.	2025-10-14	7.8
CVE-2025-24990	microsoft - multiple products	Microsoft is aware of vulnerabilities in the third party Agere Modem driver that ships natively with supported Windows operating systems. This is an announcement of the upcoming removal of ltmdm64.sys driver. The driver has been removed in the October cumulative update. Fax modem hardware dependent on this specific driver will no longer work on Windows. Microsoft recommends removing any existing dependencies on this hardware.	2025-10-14	7.8
CVE-2025-50152	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-50175	microsoft - multiple products	Use after free in Windows Digital Media allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-53150	microsoft - multiple products	Use after free in Windows Digital Media allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-53768	microsoft - multiple products	Use after free in Xbox allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55328	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.	2025-10-14	7.8
CVE-2025-55339	microsoft - multiple products	Out-of-bounds read in Windows NDIS allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55677	microsoft - multiple products	Untrusted pointer dereference in Windows Device Association Broker service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55680	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55692	microsoft - multiple products	Improper input validation in Windows Error Reporting allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55694	microsoft - multiple products	Improper access control in Windows Error Reporting allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55696	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in NtQueryInformation Token function (ntifs.h) allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55697	microsoft - multiple products	Heap-based buffer overflow in Azure Local allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-55701	microsoft - multiple products	Improper validation of specified type of input in Microsoft Windows allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-58714	microsoft - multiple products	Improper access control in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-58720	microsoft - multiple products	Use of a cryptographic primitive with a risky implementation in Windows Cryptographic Services allows an authorized attacker to disclose information locally.	2025-10-14	7.8
CVE-2025-58722	microsoft - multiple products	Heap-based buffer overflow in Windows DWM allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-58724	microsoft - azure_connected_machine_agent	Improper access control in Azure Connected Machine Agent allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-58728	microsoft - multiple products	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59187	microsoft - multiple products	Improper input validation in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59191	microsoft - multiple products	Heap-based buffer overflow in Connected Devices Platform Service (Cdpsvc) allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59192	microsoft - multiple products	Buffer over-read in Storport.sys Driver allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59199	microsoft - multiple products	Improper access control in Software Protection Platform (SPP) allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59201	microsoft - multiple products	Improper access control in Network Connection Status Indicator (NCSI) allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59207	microsoft - multiple products	Untrusted pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59222	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-10-14	7.8

CVE-2025-59223	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59224	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59225	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59226	microsoft - multiple products	Use after free in Microsoft Office Visio allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59227	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59230	microsoft - multiple products	Improper access control in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59231	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59233	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59234	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59238	microsoft - multiple products	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59241	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Health and Optimized Experiences Service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59242	microsoft - multiple products	Heap-based buffer overflow in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59243	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2025-10-14	7.8
CVE-2025-59254	microsoft - multiple products	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59255	microsoft - multiple products	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59275	microsoft - multiple products	Improper validation of specified type of input in Windows Authentication Methods allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59277	microsoft - multiple products	Improper validation of specified type of input in Windows Authentication Methods allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59278	microsoft - multiple products	Improper validation of specified type of input in Windows Authentication Methods allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59281	microsoft - xbox_gaming_services	Improper link resolution before file access ('link following') in XBox Gaming Services allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59290	microsoft - multiple products	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-59494	microsoft - azure_monitor_agent	Improper access control in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	2025-10-14	7.8
CVE-2025-54273	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.2 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.	2025-10-14	7.8
CVE-2025-54274	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.2 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.	2025-10-14	7.8
CVE-2025-54280	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.2 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.	2025-10-14	7.8
CVE-2025-54276	adobe - substance_3d_modeler	Substance3D - Modeler versions 1.22.3 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.	2025-10-14	7.8
CVE-2025-54281	adobe - multiple products	Adobe Framemaker versions 2020.9, 2022.7 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-14	7.8
CVE-2025-54282	adobe - multiple products	Adobe Framemaker versions 2020.9, 2022.7 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.	2025-10-14	7.8
CVE-2025-54283	adobe - multiple products	Illustrator versions 29.7, 28.7.9 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.	2025-10-14	7.8
CVE-2025-54284	adobe - multiple products	Illustrator versions 29.7, 28.7.9 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.	2025-10-14	7.8
CVE-2025-61798	adobe - dimension	Dimension versions 4.1.4 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.	2025-10-14	7.8
CVE-2025-61799	adobe - dimension	Dimension versions 4.1.4 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.	2025-10-14	7.8

CVE-2025-61800	adobe - dimension	Dimension versions 4.1.4 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.	2025-10-14	7.8
CVE-2025-61801	adobe - dimension	Dimension versions 4.1.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-14	7.8
CVE-2025-61802	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-14	7.8
CVE-2025-61803	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.4 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.	2025-10-14	7.8
CVE-2025-61805	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.4 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.	2025-10-14	7.8
CVE-2025-61806	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.4 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.	2025-10-14	7.8
CVE-2025-61807	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.4 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.	2025-10-14	7.8
CVE-2025-54279	adobe - multiple products	Animate versions 23.0.13, 24.0.10 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-15	7.8
CVE-2025-61804	adobe - multiple products	Animate versions 23.0.13, 24.0.10 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.	2025-10-15	7.8
CVE-2025-54268	adobe - multiple products	Bridge versions 14.1.8, 15.1.1 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.	2025-10-15	7.8
CVE-2025-54658	fortinet - fortidlp_agent	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiDLP Agent's Outlookproxy plugin for MacOS 11.5.1 and 11.4.2 through 11.4.6 and 11.3.2 through 11.3.4 and 11.2.0 through 11.2.3 and 11.1.1 through 11.1.2 and 11.0.1 and 10.5.1 and 10.4.0, and 10.3.1 may allow an authenticated attacker to escalate their privilege to Root via sending a crafted request to a local listening port.	2025-10-16	7.8
CVE-2025-53139	microsoft - multiple products	Cleartext transmission of sensitive information in Windows Hello allows an unauthorized attacker to bypass a security feature locally.	2025-10-14	7.7
CVE-2025-55698	microsoft - multiple products	Null pointer dereference in Windows DirectX allows an authorized attacker to deny service over a network.	2025-10-14	7.7
CVE-2025-59200	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Data Sharing Service Client allows an unauthorized attacker to perform spoofing locally.	2025-10-14	7.7
CVE-2025-59778	f5 - multiple products	When the Allowed IP Addresses feature is configured on the F5OS-C partition control plane, undisclosed traffic can cause multiple containers to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	7.7
CVE-2025-61884	oracle - configurator	Vulnerability in the Oracle Configurator product of Oracle E-Business Suite (component: Runtime UI). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2025-10-12	7.5
CVE-2025-25253	fortinet - multiple products	An Improper Validation of Certificate with Host Mismatch vulnerability [CWE-297] in FortiProxy version 7.6.1 and below, version 7.4.8 and below, 7.2 all versions, 7.0 all versions and FortiOS version 7.6.2 and below, version 7.4.8 and below, 7.2 all versions, 7.0 all versions ZTNA proxy may allow an unauthenticated attacker in a man-in-the middle position to intercept and tamper with connections to the ZTNA proxy	2025-10-14	7.5
CVE-2025-46774	fortinet - multiple products	An Improper Verification of Cryptographic Signature vulnerability [CWE-347] in FortiClient MacOS installer version 7.4.2 and below, version 7.2.9 and below, 7.0 all versions may allow a local user to escalate their privileges via FortiClient related executables.	2025-10-14	7.5
CVE-2025-57740	fortinet - multiple products	An Heap-based Buffer Overflow vulnerability [CWE-122] in FortiOS version 7.6.2 and below, version 7.4.7 and below, version 7.2.10 and below, 7.0 all versions, 6.4 all versions; FortiPAM version 1.5.0, version 1.4.2 and below, 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions and FortiProxy version 7.6.2 and below, version 7.4.3 and below, 7.2 all versions, 7.0 all versions RDP bookmark connection may allow an authenticated user to execute unauthorized code via crafted requests.	2025-10-14	7.5
CVE-2025-55326	microsoft - multiple products	Use after free in Connected Devices Platform Service (Cdpsvc) allows an unauthorized attacker to execute code over a network.	2025-10-14	7.5
CVE-2025-58726	microsoft - multiple products	Improper access control in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	2025-10-14	7.5
CVE-2025-59248	microsoft - multiple products	Improper input validation in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2025-10-14	7.5
CVE-2025-59502	microsoft - multiple products	Uncontrolled resource consumption in Windows Remote Procedure Call allows an unauthorized attacker to deny service over a network.	2025-10-14	7.5

CVE-2025-20350	cisco - Cisco Session Initiation Protocol (SIP) Software	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 running Cisco SIP Software could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to a buffer overflow when an affected device processes HTTP packets. An attacker could exploit this vulnerability by sending crafted HTTP input to the device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: To exploit this vulnerability, the phone must be registered to Cisco Unified Communications Manager and have Web Access enabled. Web Access is disabled by default.	2025-10-15	7.5
CVE-2025-61581	apache - traffic_control	** UNSUPPORTED WHEN ASSIGNED ** Inefficient Regular Expression Complexity vulnerability in Apache Traffic Control. This issue affects Apache Traffic Control: all versions. People with access to the management interface of the Traffic Router component could specify malicious patterns and cause unavailability. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an alternative or restrict access to the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2025-10-16	7.5
CVE-2025-41253	vmware - Spring Cloud Gateway Server Webflux	The following versions of Spring Cloud Gateway Server Webflux may be vulnerable to the ability to expose environment variables and system properties to attackers. An application should be considered vulnerable when all the following are true: * The application is using Spring Cloud Gateway Server Webflux (Spring Cloud Gateway Server WebMVC is not vulnerable). * An admin or untrusted third party using Spring Expression Language (SpEL) to access environment variables or system properties via routes. * An untrusted third party could create a route that uses SpEL to access environment variables or system properties if: * The Spring Cloud Gateway Server Webflux actuator web endpoint is enabled via management.endpoints.web.exposure.include=gateway and management.endpoint.gateway.enabled=trueor management.endpoint.gateway.access=unrestricte. * The actuator endpoints are available to attackers. * The actuator endpoints are unsecured.	2025-10-16	7.5
CVE-2025-36128	ibm - multiple products	IBM MQ 9.1, 9.2, 9.3, 9.4 LTS and 9.3, 9.4 CD is vulnerable to a denial of service, caused by improper enforcement of the timeout on individual read operations. By conducting slowloris-type attacks, a remote attacker could exploit this vulnerability to cause a denial of service.	2025-10-16	7.5
CVE-2024-33507	fortinet - fortiisolator	An insufficient session expiration vulnerability [CWE-613] and an incorrect authorization vulnerability [CWE-863] in FortiIsolator 2.4.0 through 2.4.4, 2.3 all versions, 2.2.0, 2.1 all versions, 2.0 all versions authentication mechanism may allow remote unauthenticated attacker to deauthenticate logged in admins via crafted cookie and remote authenticated read-only attacker to gain write privilege via crafted cookie.	2025-10-14	7.4
CVE-2025-48004	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	2025-10-14	7.4
CVE-2025-55335	microsoft - multiple products	Use after free in Windows NTFS allows an unauthorized attacker to elevate privileges locally.	2025-10-14	7.4
CVE-2025-55687	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Resilient File System (ReFS) allows an unauthorized attacker to elevate privileges locally.	2025-10-14	7.4
CVE-2025-55693	microsoft - multiple products	Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.	2025-10-14	7.4
CVE-2025-59189	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	2025-10-14	7.4
CVE-2025-59206	microsoft - multiple products	Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability	2025-10-14	7.4
CVE-2025-59210	microsoft - multiple products	Windows Resilient File System (ReFS) Deduplication Service Elevation of Privilege Vulnerability	2025-10-14	7.4
CVE-2025-40809	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds write vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	2025-10-14	7.3
CVE-2025-40810	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds write vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	2025-10-14	7.3
CVE-2025-40811	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	2025-10-14	7.3
CVE-2025-40812	siemens - multiple products	A vulnerability has been identified in Solid Edge SE2024 (All versions < V224.0 Update 14), Solid Edge SE2025 (All versions < V225.0 Update 6). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PRT files. This could allow an attacker to crash the application or execute code in the context of the current process.	2025-10-14	7.3
CVE-2025-25004	microsoft - multiple products	Improper access control in Microsoft PowerShell allows an authorized attacker to elevate privileges locally.	2025-10-14	7.3
CVE-2025-55240	microsoft - multiple products	Improper access control in Visual Studio allows an authorized attacker to elevate privileges locally.	2025-10-14	7.3
CVE-2025-55247	microsoft - multiple products	Improper link resolution before file access ('link following') in .NET allows an authorized attacker to elevate privileges locally.	2025-10-14	7.3
CVE-2025-49552	adobe - connect	Adobe Connect versions 12.9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by a high-privileged attacker to execute malicious scripts in a victim's browser. Exploitation of this issue requires user interaction in that a victim must navigate to a crafted web page. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality and integrity impact as high. Scope is changed.	2025-10-14	7.3

CVE-2025-47856	fortinet - multiple products	Two improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerabilities [CWE-78] in Fortinet FortiVoice version 7.2.0, 7.0.0 through 7.0.6 and before 6.4.10 allows a privileged attacker to execute arbitrary code or commands via crafted HTTP/HTTPS or CLI requests.	2025-10-14	7.2
CVE-2025-10242	ivanti - multiple products	OS command injection in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2025-10-14	7.2
CVE-2025-10243	ivanti - multiple products	OS command injection in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2025-10-14	7.2
CVE-2025-10985	ivanti - multiple products	OS command injection in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2025-10-14	7.2
CVE-2024-50571	fortinet - multiple products	A heap-based buffer overflow in Fortinet FortiOS 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.10, 7.0.0 through 7.0.16, 6.4.0 through 6.4.15, 6.2.0 through 6.2.17, FortiManager Cloud 7.6.2, 7.4.1 through 7.4.5, 7.2.1 through 7.2.8, 7.0.1 through 7.0.13, 6.4.1 through 6.4.7, FortiAnalyzer Cloud 7.4.1 through 7.4.5, 7.2.1 through 7.2.8, 7.0.1 through 7.0.13, 6.4.1 through 6.4.7, FortiProxy 7.6.0, 7.4.0 through 7.4.6, 7.2.0 through 7.2.12, 7.0.0 through 7.0.19, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiAnalyzer 7.6.0 through 7.6.2, 7.4.0 through 7.4.5, 7.2.0 through 7.2.8, 7.0.0 through 7.0.13, 6.4.0 through 6.4.15, 6.2.0 through 6.2.13, 6.0.0 through 6.0.12, FortiManager 7.6.0 through 7.6.1, 7.4.0 through 7.4.5, 7.2.0 through 7.2.9, 7.0.0 through 7.0.13, 6.4.0 through 6.4.15, 6.2.0 through 6.2.13, 6.0.0 through 6.0.12 allows attacker to execute unauthorized code or commands via specifically crafted requests.	2025-10-14	7.2
CVE-2025-37132	hewlett packard enterprise (hpe) - ArubaOS (AOS)	An arbitrary file write vulnerability exists in the web-based management interface of both the AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to upload arbitrary files and execute arbitrary commands on the underlying operating system.	2025-10-14	7.2
CVE-2025-37133	hewlett packard enterprise (hpe) - ArubaOS (AOS)	An authenticated command injection vulnerability exists in the CLI binary of an AOS-8 Controller/Mobility Conductor operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	2025-10-14	7.2
CVE-2025-37134	hewlett packard enterprise (hpe) - ArubaOS (AOS)	An authenticated command injection vulnerability exists in the CLI binary of an AOS-8 Controller/Mobility Conductor operating system. Successful exploitation could allow an authenticated malicious actor to execute arbitrary commands as a privileged user on the underlying operating system.	2025-10-14	7.2
CVE-2025-37146	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the web-based management interface of network access point configuration services could allow an authenticated remote attacker to perform remote command execution. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.	2025-10-14	7.2
CVE-2025-37147	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A Secure Boot Bypass Vulnerability exists in affected Access Points that allows an adversary to bypass the hardware root of trust verification in place to ensure only vendor-signed firmware can execute on the device. An adversary can exploit this vulnerability to run modified or custom firmware on affected Access Points.	2025-10-14	7.1
CVE-2025-59208	microsoft - multiple products	Out-of-bounds read in Windows MapUrlToZone allows an unauthorized attacker to disclose information over a network.	2025-10-14	7.1
CVE-2025-59232	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2025-10-14	7.1
CVE-2025-59235	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2025-10-14	7.1
CVE-2025-47148	f5 - multiple products	When the BIG-IP system is configured as both a Security Assertion Markup Language (SAML) service provider (SP) and Identity Provider (IdP), with single logout (SLO) enabled on an access policy, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	7.1
CVE-2025-47150	f5 - multiple products	When SNMP is configured on F5OS Appliance and Chassis systems, undisclosed requests can cause an increase in SNMP memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	7.1
CVE-2025-55670	f5 - multiple products	On BIG-IP Next CNF, BIG-IP Next SPK, and BIG-IP Next for Kubernetes systems, repeated undisclosed API calls can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	7.1
CVE-2025-40772	siemens - sipass_integrated	A vulnerability has been identified in SiPass integrated (All versions < V3.0). Affected server applications are vulnerable to stored Cross-Site Scripting (XSS), allowing an attacker to inject malicious code that can be executed by other users when they visit the affected page. Successful exploitation allows an attacker to impersonate other users within the application and steal their session data. This could enable unauthorized access to accounts and potentially lead to privilege escalation.	2025-10-14	7.0
CVE-2024-48891	fortinet - multiple products	An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiSOAR 7.6.0 through 7.6.1, 7.5.0 through 7.5.1, 7.4 all versions, 7.3 all versions may allow an attacker who has already obtained a non-login low privileged shell access (via another hypothetical vulnerability) to perform a local privilege escalation via crafted commands.	2025-10-14	7.0
CVE-2025-47989	microsoft - azure_connected_machine_agent	Improper access control in Azure Connected Machine Agent allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-50174	microsoft - multiple products	Use after free in Windows Device Association Broker service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-53717	microsoft - multiple products	Reliance on untrusted inputs in a security decision in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55331	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0

CVE-2025-55340	microsoft - multiple products	Improper authentication in Windows Remote Desktop Protocol allows an authorized attacker to bypass a security feature locally.	2025-10-14	7.0
CVE-2025-55678	microsoft - multiple products	Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55681	microsoft - multiple products	Out-of-bounds read in Windows DWM allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55684	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55685	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55686	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55688	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55689	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55690	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-55691	microsoft - multiple products	Use after free in Windows PrintWorkflowUserSvc allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-58725	microsoft - multiple products	Heap-based buffer overflow in Windows COM allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-58727	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Connected Devices Platform Service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-58730	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58731	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58732	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58733	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58734	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58735	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58736	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58737	microsoft - multiple products	Use after free in Windows Remote Desktop allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-58738	microsoft - multiple products	Use after free in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-59193	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59194	microsoft - multiple products	Use of uninitialized resource in Windows Kernel allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59195	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to deny service locally.	2025-10-14	7.0
CVE-2025-59196	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59202	microsoft - multiple products	Use after free in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59205	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.	2025-10-14	7.0
CVE-2025-59221	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-59261	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59282	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Inbox COM Objects allows an unauthorized attacker to execute code locally.	2025-10-14	7.0
CVE-2025-59285	microsoft - azure_monitor_agent	Deserialization of untrusted data in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59289	microsoft - multiple products	Double free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-10-14	7.0
CVE-2025-59497	microsoft - defender_for_endpoint	Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Linux allows an authorized attacker to deny service locally.	2025-10-14	7.0
CVE-2025-54755	f5 - multiple products	A directory traversal vulnerability exists in TMUI that allows an authenticated attacker to access files which are not limited to the intended files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	6.9
CVE-2025-58474	f5 - multiple products	When BIG-IP Advanced WAF is configured on a virtual server with Server-Side Request Forgery (SSRF) protection or when an NGINX server is configured with App Protect Bot Defense, undisclosed requests can disrupt new client requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	6.9
CVE-2025-59268	f5 - multiple products	On the BIG-IP system, undisclosed endpoints that contain static non-sensitive information are accessible to an unauthenticated remote attacker through the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	6.9

CVE-2025-60015	f5 - multiple products	An out-of-bounds write vulnerability exists in F5OS-A and F5OS-C that could lead to memory corruption. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	6.9
CVE-2025-34254	d-link - Nuclias Connect	D-Link Nuclias Connect firmware versions <= 1.3.1.4 contain an observable response discrepancy vulnerability. The application's 'Login' endpoint returns distinct JSON responses depending on whether the supplied username is associated with an existing account. Because the responses differ in the `error.message`string value, an unauthenticated remote attacker can enumerate valid usernames/accounts on the server. NOTE: D-Link states that a fix is under development.	2025-10-16	6.9
CVE-2025-34255	d-link - Nuclias Connect	D-Link Nuclias Connect firmware versions <= 1.3.1.4 contain an observable response discrepancy vulnerability. The application's 'Forgot Password' endpoint returns distinct JSON responses depending on whether the supplied email address is associated with an existing account. Because the responses differ in the `data.exist` boolean value, an unauthenticated remote attacker can enumerate valid email addresses/accounts on the server. NOTE: D-Link states that a fix is under development.	2025-10-16	6.9
CVE-2025-55320	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Configuration Manager allows an authorized attacker to elevate privileges over an adjacent network.	2025-10-14	6.8
CVE-2025-9548	lenovo - Power Management Driver	A potential null pointer dereference vulnerability was reported in the Lenovo Power Management Driver that could allow a local authenticated user to cause a Windows blue screen error.	2025-10-15	6.8
CVE-2025-40774	siemens - sipass_integrated	A vulnerability has been identified in SiPass integrated (All versions < V3.0). Affected server applications store user passwords encrypted in its database. Decryption keys are accessible to users with administrative privileges, allowing them to recover passwords. Successful exploitation of this vulnerability allows an attacker to obtain and use valid user passwords. This can lead to unauthorized access to user accounts, data breaches, and potential system compromise.	2025-10-14	6.7
CVE-2023-46718	fortinet - multiple products	A stack-based buffer overflow in Fortinet FortiOS version 7.4.0 through 7.4.1 and 7.2.0 through 7.2.7 and 7.0.0 through 7.0.12 and 6.4.6 through 6.4.15 and 6.2.9 through 6.2.16 and 6.0.13 through 6.0.18 allows attacker to execute unauthorized code or commands via specially crafted CLI commands.	2025-10-14	6.7
CVE-2025-57716	fortinet - multiple products	An Uncontrolled Search Path Element vulnerability [CWE-427] in FortiClient Windows 7.4.0 through 7.4.3, 7.2.0 through 7.2.11, 7.0 all versions may allow a local low privileged user to perform a DLL hijacking attack via placing a malicious DLL to the FortiClient Online Installer installation folder.	2025-10-14	6.7
CVE-2025-33096	ibm - multiple products	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user to cause a denial of service by uploading specially crafted files using uncontrolled recursion.	2025-10-12	6.5
CVE-2025-11623	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62383	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62384	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62385	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62386	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62387	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62388	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62389	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62390	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62391	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-62392	ivanti - multiple products	SQL injection in Ivanti Endpoint Manager allows a remote authenticated attacker to read arbitrary data from the database.	2025-10-13	6.5
CVE-2025-11711	mozilla - multiple products	There was a way to change the value of JavaScript Object properties that were supposed to be non-writeable. This vulnerability affects Firefox < 144, Firefox ESR < 115.29, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	6.5
CVE-2025-11716	mozilla - multiple products	Links in a sandboxed iframe could open an external app on Android without the required "allow-" permission. This vulnerability affects Firefox < 144 and Thunderbird < 144.	2025-10-14	6.5
CVE-2025-11718	mozilla - firefox	When the address bar was hidden due to scrolling on Android, a malicious page could create a fake address bar to fool the user in response to a visibilitychange event This vulnerability affects Firefox < 144.	2025-10-14	6.5
CVE-2025-22258	fortinet - multiple products	A heap-based buffer overflow in Fortinet FortiSRA 1.5.0, 1.4.0 through 1.4.2, FortiPAM 1.5.0, 1.4.0 through 1.4.2, 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiProxy 7.6.0 through 7.6.1, 7.4.0 through 7.4.7, FortiOS 7.6.0 through 7.6.2, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10, 7.0.2 through 7.0.16, FortiSwitchManager 7.2.1 through 7.2.5 allows attackers to escalate their privilege via specially crafted http requests.	2025-10-14	6.5
CVE-2025-53845	fortinet - multiple products	An improper authentication vulnerability [CWE-287] in Fortinet FortiAnalyzer version 7.6.0 through 7.6.3 and before 7.4.6 allows an unauthenticated attacker to obtain information pertaining to the device's health and status, or cause a denial of service via crafted OFTP requests.	2025-10-14	6.5
CVE-2025-59921	fortinet - multiple products	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in Fortinet FortiADC version 7.4.0, version 7.2.3 and below, version 7.1.4 and below, 7.0 all versions, 6.2 all versions may allow an authenticated attacker to obtain sensitive data via crafted HTTP or HTTPs requests.	2025-10-14	6.5

CVE-2025-37135	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file deletion vulnerabilities have been identified in the command-line interface of an AOS-8 Controller/Mobility Conductor. Successful exploitation of these vulnerabilities could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	2025-10-14	6.5
CVE-2025-37136	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file deletion vulnerabilities have been identified in the command-line interface of an AOS-8 Controller/Mobility Conductor. Successful exploitation of these vulnerabilities could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	2025-10-14	6.5
CVE-2025-37137	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file deletion vulnerabilities have been identified in the command-line interface of an AOS-8 Controller/Mobility Conductor. Successful exploitation of these vulnerabilities could allow an authenticated remote malicious actor to delete arbitrary files within the affected system.	2025-10-14	6.5
CVE-2025-37148	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the parsing of ethernet frames in AOS-8 Instant and AOS 10 could allow an unauthenticated remote attacker to conduct a denial of service attack. Successful exploitation could allow an attacker to potentially disrupt network services and require manual intervention to restore functionality.	2025-10-14	6.5
CVE-2025-55700	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.	2025-10-14	6.5
CVE-2025-58717	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.	2025-10-14	6.5
CVE-2025-58729	microsoft - multiple products	Improper validation of specified type of input in Windows Local Session Manager (LSM) allows an authorized attacker to deny service over a network.	2025-10-14	6.5
CVE-2025-58739	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.	2025-10-14	6.5
CVE-2025-59185	microsoft - multiple products	External control of file name or path in Windows Core Shell allows an unauthorized attacker to perform spoofing over a network.	2025-10-14	6.5
CVE-2025-59214	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.	2025-10-14	6.5
CVE-2025-59244	microsoft - multiple products	External control of file name or path in Windows Core Shell allows an unauthorized attacker to perform spoofing over a network.	2025-10-14	6.5
CVE-2025-59257	microsoft - multiple products	Improper validation of specified type of input in Windows Local Session Manager (LSM) allows an authorized attacker to deny service over a network.	2025-10-14	6.5
CVE-2025-59259	microsoft - multiple products	Improper validation of specified type of input in Windows Local Session Manager (LSM) allows an authorized attacker to deny service over a network.	2025-10-14	6.5
CVE-2025-54267	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 Incorrect Authorization vulnerability. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized access to elevated privileges that increase integrity impact to high. Exploitation of this issue does not require user interaction.	2025-10-14	6.5
CVE-2025-55039	apache - multiple products	This issue affects Apache Spark versions before 3.4.4, 3.5.2 and 4.0.0. Apache Spark versions before 4.0.0, 3.5.2 and 3.4.4 use an insecure default network encryption cipher for RPC communication between nodes. When spark.network.crypto.enabled is set to true (it is set to false by default), but spark.network.crypto.cipher is not explicitly configured, Spark defaults to AES in CTR mode (AES/CTR/NoPadding), which provides encryption without authentication. This vulnerability allows a man-in-the-middle attacker to modify encrypted RPC traffic undetected by flipping bits in ciphertext, potentially compromising heartbeat messages or application data and affecting the integrity of Spark workflows. To mitigate this issue, users should either configure spark.network.crypto.cipher to AES/GCM/NoPadding to enable authenticated encryption or enable SSL encryption by setting spark.ssl.enabled to true, which provides stronger transport security.	2025-10-15	6.5
CVE-2025-20359	cisco - multiple products	Multiple Cisco products are affected by a vulnerability in the Snort 3 HTTP Decoder that could allow an unauthenticated, remote attacker to cause the disclosure of possible sensitive data or cause the Snort 3 Detection Engine to crash. This vulnerability is due to an error in the logic of buffer handling when the MIME fields of the HTTP header are parsed. This can result in a buffer under-read. An attacker could exploit this vulnerability by sending crafted HTTP packets through an established connection that is parsed by Snort 3. A successful exploit could allow the attacker to induce one of two possible outcomes: the unexpected restarting of the Snort 3 Detection Engine, which could cause a denial of service (DoS) condition, or information disclosure of sensitive information in the Snort 3 data stream. Due to the under-read condition, it is possible that sensitive information that is not valid connection data could be returned.	2025-10-15	6.5
CVE-2025-58324	fortinet - fortisiem	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiSIEM 7.2.0 through 7.2.2, 7.1 all versions, 7.0 all versions, 6.7 all versions, 6.6 all versions, 6.5 all versions, 6.4 all versions, 6.3 all versions, 6.2 all versions may allow an authenticated attacker to perform a stored cross site scripting (XSS) attack via crafted HTTP requests.	2025-10-14	6.4
CVE-2025-43991	dell - multiple products	SupportAssist for Home PCs versions 4.8.2 and prior and SupportAssist for Business PCs versions 4.5.3 and prior, contain an UNIX Symbolic Link (Symlink) following vulnerability. A low privileged attacker with local access to the system could potentially exploit this vulnerability to delete arbitrary files only in that affected system.	2025-10-13	6.3
CVE-2025-48813	microsoft - multiple products	Use of a key past its expiration date in Virtual Secure Mode allows an authorized attacker to perform spoofing locally.	2025-10-14	6.3
CVE-2025-58424	f5 - multiple products	On BIG-IP systems, undisclosed traffic can cause data corruption and unauthorized data modification in protocols which do not have message integrity protection. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	6.3
CVE-2025-37138	hewlett packard enterprise (hpe) - ArubaOS (AOS)	An authenticated command injection vulnerability exists in the command line interface binary of AOS-10 GW and AOS-8 Controllers/Mobility Conductor operating system. Exploitation of this vulnerability requires physical access to the hardware controllers. A successful attack could allow an authenticated malicious actor with physical access to execute arbitrary commands as a privileged user on the underlying operating system.	2025-10-14	6.2
CVE-2025-55334	microsoft - multiple products	Cleartext storage of sensitive information in Windows Kernel allows an unauthorized attacker to bypass a security feature locally.	2025-10-14	6.2
CVE-2025-59258	microsoft - multiple products	Insertion of sensitive information into log file in Active Directory Federation Services allows an unauthorized attacker to disclose information locally.	2025-10-14	6.2

CVE-2025-11712	mozilla - multiple products	A malicious page could have used the type attribute of an OBJECT tag to override the default browser behavior when encountering a web resource served without a content-type. This could have contributed to an XSS on a site that unsafely serves files without a content-type header. This vulnerability affects Firefox < 144, Firefox ESR < 140.4, Thunderbird < 144, and Thunderbird < 140.4.	2025-10-14	6.1
CVE-2024-44088	apache - geode	Malicious script injection ('Cross-site Scripting') vulnerability in Apache Geode web-api (REST). This vulnerability allows an attacker that tricks a logged-in user into clicking a specially-crafted link to execute code on the returned page, which could lead to theft of the user's session information and even account takeover. This issue affects Apache Geode: all versions prior to 1.15.2 Users are recommended to upgrade to version 1.15.2, which fixes the issue.	2025-10-14	6.1
CVE-2025-55330	microsoft - multiple products	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-10-14	6.1
CVE-2025-55332	microsoft - multiple products	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-10-14	6.1
CVE-2025-55333	microsoft - multiple products	Incomplete comparison with missing factors in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-10-14	6.1
CVE-2025-55337	microsoft - multiple products	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-10-14	6.1
CVE-2025-55338	microsoft - multiple products	Missing Ability to Patch ROM Code in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-10-14	6.1
CVE-2025-55682	microsoft - multiple products	Improper enforcement of behavioral workflow in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2025-10-14	6.1
CVE-2025-20351	cisco - Cisco Session Initiation Protocol (SIP) Software	A vulnerability in the web UI of Cisco Desk Phone 9800 Series, Cisco IP Phone 7800 and 8800 Series, and Cisco Video Phone 8875 running Cisco SIP Software could allow an unauthenticated, remote attacker to conduct XSS attacks against a user of the web UI. This vulnerability exists because the web UI of an affected device does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Note: To exploit this vulnerability, the phone must be registered to Cisco Unified Communications Manager and have Web Access enabled. Web Access is disabled by default.	2025-10-15	6.1
CVE-2025-37149	hewlett packard enterprise (hpe) - ProLiant RL300 Gen11 Server	A potential out-of-bound reads vulnerability in HPE ProLiant RL300 Gen11 Server's UEFI firmware.	2025-10-14	6.0
CVE-2025-37139	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in an AOS firmware binary allows an authenticated malicious actor to permanently delete necessary boot information. Successful exploitation may render the system unbootable, resulting in a Denial of Service that can only be resolved by replacing the affected hardware.	2025-10-14	6.0
CVE-2025-54805	f5 - multiple products	When an iRule is configured on a virtual server via the declarative API, upon re-instantiation, the cleanup process can cause an increase in the Traffic Management Microkernel (TMM) memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	6.0
CVE-2025-10699	lenovo - LeCloud Client	A vulnerability was reported in the Lenovo LeCloud client application that, under certain conditions, could allow information disclosure.	2025-10-15	6.0
CVE-2025-54265	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 Incorrect Authorization vulnerability. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction.	2025-10-14	5.9
CVE-2025-31365	fortinet - multiple products	An Improper Control of Generation of Code ('Code Injection') vulnerability [CWE-94] in FortiClientMac 7.4.0 through 7.4.3, 7.2.1 through 7.2.8 may allow an unauthenticated attacker to execute arbitrary code on the victim's host via tricking the user into visiting a malicious website.	2025-10-14	5.8
CVE-2025-20360	cisco - multiple products	Multiple Cisco products are affected by a vulnerability in the Snort 3 HTTP Decoder that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to restart. This vulnerability is due to a lack of complete error checking when the MIME fields of the HTTP header are parsed. An attacker could exploit this vulnerability by sending crafted HTTP packets through an established connection to be parsed by Snort 3. A successful exploit could allow the attacker to cause a DoS condition when the Snort 3 Detection Engine unexpectedly restarts.	2025-10-15	5.8
CVE-2025-2140	ibm - multiple products	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user on the network to spoof email identity of the sender due to improper verification of source data.	2025-10-12	5.7
CVE-2025-9955	wso2 - multiple products	An improper access control vulnerability exists in WSO2 Enterprise Integrator product due to insufficient permission restrictions on internal SOAP admin services related to system logs and user-store configuration. A low-privileged user can access log data and user-store configuration details that are not intended to be exposed at that privilege level. While no credentials or sensitive user information are exposed, this vulnerability may allow unauthorized visibility into internal operational details, which could aid in further exploitation or reconnaissance.	2025-10-16	5.7
CVE-2025-53860	f5 - multiple products	A vulnerability exists in F5OS-A software that allows a highly privileged authenticated attacker to access sensitive FIPS hardware security module (HSM) information on F5 rSeries systems. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	5.6
CVE-2025-54271	adobe - creative_cloud	Creative Cloud Desktop versions 6.7.0.278 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to arbitrary file system write. A low-privileged attacker could exploit the timing between the check and use of a resource, potentially allowing unauthorized modifications to files. Exploitation of this issue does not require user interaction.	2025-10-15	5.6
CVE-2025-47979	microsoft - multiple products	Insertion of sensitive information into log file in Windows Failover Cluster allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-55325	microsoft - multiple products	Buffer over-read in Windows Storage Management Provider allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-55336	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Cloud Files Mini Filter Driver allows an authorized attacker to disclose information locally.	2025-10-14	5.5

CVE-2025-55676	microsoft - multiple products	Generation of error message containing sensitive information in Windows USB Video Driver allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-55683	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-55695	microsoft - multiple products	Out-of-bounds read in Windows WLAN Auto Config Service allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-55699	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59184	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows High Availability Services allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59186	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59188	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Failover Cluster allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59190	microsoft - multiple products	Improper input validation in Microsoft Windows Search Component allows an unauthorized attacker to deny service locally.	2025-10-14	5.5
CVE-2025-59197	microsoft - multiple products	Insertion of sensitive information into log file in Windows ETL Channel allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59203	microsoft - multiple products	Insertion of sensitive information into log file in Windows StateRepository API allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59204	microsoft - multiple products	Use of uninitialized resource in Windows Management Services allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59209	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Push Notification Core allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59211	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Push Notification Core allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-59229	microsoft - multiple products	Uncaught exception in Microsoft Office allows an unauthorized attacker to deny service locally.	2025-10-14	5.5
CVE-2025-59253	microsoft - multiple products	Improper access control in Microsoft Windows Search Component allows an authorized attacker to deny service locally.	2025-10-14	5.5
CVE-2025-59260	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Microsoft Failover Cluster Virtual Driver allows an authorized attacker to disclose information locally.	2025-10-14	5.5
CVE-2025-54275	adobe - substance_3d_viewer	Substance3D - Viewer versions 0.25.2 and earlier are affected by an out-of-bounds write vulnerability that could lead to application denial-of-service. An attacker could leverage this vulnerability to crash the application or make it unavailable. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-14	5.5
CVE-2025-54269	adobe - multiple products	Animate versions 23.0.13, 24.0.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-15	5.5
CVE-2025-54270	adobe - multiple products	Animate versions 23.0.13, 24.0.10 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive memory information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-15	5.5
CVE-2025-54278	adobe - multiple products	Bridge versions 14.1.8, 15.1.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-10-15	5.5
CVE-2025-43282	apple - multiple products	A double free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.6, iOS 18.6 and iPadOS 18.6, watchOS 11.6, tvOS 18.6, visionOS 2.6, macOS Ventura 13.7.7, macOS Sonoma 14.7.7, iPadOS 17.7.9. An app may be able to cause unexpected system termination.	2025-10-15	5.5
CVE-2025-43313	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.7.7, macOS Sonoma 14.7.7, macOS Sequoia 15.6. An app may be able to access sensitive user data.	2025-10-15	5.5
CVE-2025-53950	fortinet - fortidlp_agent	An Exposure of Private Personal Information ('Privacy Violation') vulnerability [CWE-359] in Fortinet FortiDLP Agent's Outlookproxy plugin for MacOS and Windows 11.5.1 and 11.4.2 through 11.4.6 and 11.3.2 through 11.3.4 and 11.2.0 through 11.2.3 and 11.1.1. through 11.1.2 and 11.0.1 and 10.5.1 and 10.4.0, and 10.3.1 may allow an authenticated administrator to collect current user's email information.	2025-10-16	5.5
CVE-2025-36002	ibm - multiple products	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5, and 6.2.1.0 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5, and 6.2.1.0 stores user credentials in configuration files which can be read by a local user.	2025-10-16	5.5
CVE-2025-54272	adobe - Adobe Experience Manager	Adobe Experience Manager versions 11.6 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. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	2025-10-14	5.4
CVE-2025-61796	adobe - Adobe Experience Manager	Adobe Experience Manager versions 11.6 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. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	2025-10-14	5.4
CVE-2025-61797	adobe - Adobe Experience Manager	Adobe Experience Manager versions 11.6 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. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	2025-10-14	5.4

CVE-2025-62243	liferay - multiple products	Insecure direct object reference (IDOR) vulnerability in Publications in Liferay Portal 7.4.1 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote authenticated attackers to view publication comments via the _com_liferay_change_tracking_web_portlet_PublicationsPortlet_value parameter. Publications comments in Liferay Portal 7.4.1 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 does not properly check user permissions, which allows remote authenticated users to edit publication comments via crafted URLs.	2025-10-13	5.3
CVE-2025-62241	liferay - DXP	Insecure Direct Object Reference (IDOR) vulnerability with shipment addresses in Liferay DXP 2023.Q4.1 through 2023.Q4.5 allows remote authenticated users to from one virtual instance to view the shipment addresses of different virtual instance via the _com_liferay_commerce_order_web_internal_portlet_CommerceOrderPortlet_commerceOrderId parameter.	2025-10-13	5.3
CVE-2025-62242	liferay - multiple products	Insecure Direct Object Reference (IDOR) vulnerability with account addresses in Liferay Portal 7.4.3.4 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92 allows remote authenticated users to from one account to view addresses from a different account via the _com_liferay_account_admin_web_internal_portlet_AccountEntriesAdminPortlet_addressId parameter.	2025-10-13	5.3
CVE-2025-62252	liferay - multiple products	Insecure Direct Object Reference (IDOR) vulnerability in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows remote authenticated users in one virtual instance to assign an organization to a user in a different virtual instance via the _com_liferay_users_admin_web_portlet_UsersAdminPortlet_addUserIds parameter.	2025-10-13	5.3
CVE-2025-27906	ibm - multiple products	IBM Content Navigator 3.0.11, 3.0.15, 3.1.0, and 3.2.0 could expose the directory listing of the application upon using an application URL. Application files and folders are visible in the browser to a user; however, the contents of the files cannot be read obtained or modified.	2025-10-14	5.3
CVE-2024-26008	fortinet - multiple products	An improper check or handling of exceptional conditions vulnerability [CWE-703] in FortiOS version 7.4.0 through 7.4.3 and before 7.2.7, FortiProxy version 7.4.0 through 7.4.3 and before 7.2.9, FortiPAM before 1.2.0 and FortiSwitchManager version 7.2.0 through 7.2.3 and version 7.0.0 through 7.0.3 fgfm daemon may allow an unauthenticated attacker to repeatedly reset the fgfm connection via crafted SSL encrypted TCP requests.	2025-10-14	5.3
CVE-2025-54973	fortinet - multiple products	A concurrent execution using shared resource with improper synchronization ('Race Condition') vulnerability [CWE-362] in Fortinet FortiAnalyzer version 7.6.0 through 7.6.2, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10 and before 7.0.13 allows an attacker to attempt to win a race condition to bypass the FortiCloud SSO authorization via crafted FortiCloud SSO requests.	2025-10-14	5.3
CVE-2025-59288	microsoft - playwright	Improper verification of cryptographic signature in GitHub allows an unauthorized attacker to perform spoofing over an adjacent network.	2025-10-14	5.3
CVE-2025-58133	zoom - multiple products	Authentication bypass in some Zoom Rooms Clients before version 6.5.1 may allow an unauthenticated user to conduct a disclosure of information via network access.	2025-10-15	5.3
CVE-2025-53951	fortinet - fortidlp_agent	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability [CWE-22] in Fortinet FortiDLP Agent's Outlookproxy plugin for Windows 11.5.1 and 11.4.2 through 11.4.6 and 11.3.2 through 11.3.4 and 11.2.0 through 11.2.3 and 11.1.1 through 11.1.2 and 11.0.1 and 10.5.1 and 10.4.0, and 10.3.1 may allow an authenticated attacker to escalate their privilege to LocalService via sending a crafted request to a local listening port.	2025-10-16	5.3
CVE-2025-11665	d-link - DAP-2695	A vulnerability was detected in D-Link DAP-2695 2.00RC131. This affects the function fwupdater_main of the file rgbin of the component Firmware Update Handler. Performing manipulation results in os command injection. The attack may be initiated remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2025-10-13	5.1
CVE-2025-40773	siemens - sipass_integrated	A vulnerability has been identified in SiPass integrated (All versions < V3.0). Affected server applications contains a broken access control vulnerability. The authorization mechanism lacks sufficient server-side checks, allowing an attacker to execute a specific API request. Successful exploitation allows an attacker to potentially manipulate data belonging to other users.	2025-10-14	5.1
CVE-2025-55679	microsoft - multiple products	Improper input validation in Windows Kernel allows an unauthorized attacker to disclose information locally.	2025-10-14	5.1
CVE-2025-61933	f5 - multiple products	A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of BIG-IP APM that allows an attacker to run JavaScript in the context of the targeted logged-out user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	5.1
CVE-2025-34253	d-link - Nuclias Connect	D-Link Nuclias Connect firmware versions <= 1.3.1.4 contain a stored cross-site scripting (XSS) vulnerability due to improper sanitization of the 'Network' field when editing the configuration, creating a profile, and adding a network. An authenticated attacker can inject arbitrary JavaScript to be executed in the context of other users viewing the profile entry. NOTE: D-Link states that a fix is under development.	2025-10-16	5.1
CVE-2025-59198	microsoft - multiple products	Improper input validation in Microsoft Windows Search Component allows an authorized attacker to deny service locally.	2025-10-14	5
CVE-2025-37140	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file download vulnerabilities exist in the CLI binary of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	2025-10-14	4.9
CVE-2025-37141	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file download vulnerabilities exist in the CLI binary of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	2025-10-14	4.9
CVE-2025-37142	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file download vulnerabilities exist in the CLI binary of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	2025-10-14	4.9
CVE-2025-37143	hewlett packard enterprise (hpe) - ArubaOS (AOS)	An arbitrary file download vulnerability exists in the web-based management interface of AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an Authenticated malicious actor to download arbitrary files through carefully constructed exploits.	2025-10-14	4.9

CVE-2025-37144	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file download vulnerabilities exist in a low-level interface library in AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	2025-10-14	4.9
CVE-2025-37145	hewlett packard enterprise (hpe) - ArubaOS (AOS)	Arbitrary file download vulnerabilities exist in a low-level interface library in AOS-10 GW and AOS-8 Controller/Mobility Conductor operating systems. Successful exploitation could allow an authenticated malicious actor to download arbitrary files through carefully constructed exploits.	2025-10-14	4.9
CVE-2025-20329	cisco - Cisco RoomOS Software	A vulnerability in the logging component of Cisco TelePresence Collaboration Endpoint (CE) and Cisco RoomOS Software could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability exists because certain unencrypted credentials are stored when SIP media component logging is enabled. An attacker could exploit this vulnerability by accessing the audit logs on an affected system and obtaining credentials to which they may not normally have access. A successful exploit could allow the attacker to use those credentials to access confidential information, some of which may contain personally identifiable information (PII). Note: To access the logs that are stored in the Webex Cloud or stored on the device itself, an attacker must have valid administrative credentials.	2025-10-15	4.9
CVE-2025-62244	liferay - multiple products	Insecure direct object reference (IDOR) vulnerability in Publications in Liferay Portal 7.3.1 through 7.4.3.111, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, and 7.4 GA through update 92, and 7.3 GA through update 36 allows remote authenticated attackers to view the edit page of a publication via the _com_liferay_change_tracking_web_portlet_PublicationsPortlet_ctCollectionId parameter.	2025-10-13	4.8
CVE-2025-62246	liferay - multiple products	Multiple stored cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.5, 2023.Q3.1 through 2023.Q3.8, 7.4 GA through update 92, and older unsupported versions allow remote authenticated users to inject arbitrary web script or HTML via a crafted payload injected into a user's first, middle or last name text field to (1) page comments widget, (2) blog entry comments, (3) document and media document comments, (4) message board messages, (5) wiki page comments or (6) other widgets/apps that supports mentions.	2025-10-13	4.8
CVE-2025-62251	liferay - multiple products	Liferay Portal 7.3.0 through 7.4.3.119, and Liferay DXP 2023.Q3.1 through 2023.Q3.8, 2023.Q4.0 through 2023.Q4.5, 7.4 GA through update 92 and 7.3 GA though update 36 shows content to users who do not have permission to view it via the Menu Display Widget. This security flaw could result in sensitive information being exposed to unauthorized users.	2025-10-13	4.8
CVE-2025-25252	fortinet - multiple products	An Insufficient Session Expiration vulnerability [CWE-613] in FortiOS SSL VPN 7.6.0 through 7.6.2, 7.4.0 through 7.4.6, 7.2.0 through 7.2.10, 7.0.0 through 7.0.16, 6.4 all versions may allow a remote attacker (e.g. a former admin whose account was removed and whose session was terminated) in possession of the SAML record of a user session to access or re-open that session via re-use of SAML record.	2025-10-14	4.8
CVE-2025-55248	microsoft - multiple products	Inadequate encryption strength in .NET, .NET Framework, Visual Studio allows an authorized attacker to disclose information over a network.	2025-10-14	4.8
CVE-2025-54266	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 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. Exploitation of this issue requires user interaction in that a victim must browse to the page containing the vulnerable field. Scope is changed.	2025-10-14	4.8
CVE-2025-11839	gnu - binutils	A security flaw has been discovered in GNU Binutils 2.45. Impacted is the function tg_tag_type of the file prdbg.c. Performing manipulation results in unchecked return value. The attack needs to be approached locally. The exploit has been released to the public and may be exploited.	2025-10-16	4.8
CVE-2025-11840	gnu - binutils	A weakness has been identified in GNU Binutils 2.45. The affected element is the function vfinfo of the file ldmisc.c. Executing manipulation can lead to out-of-bounds read. The attack can only be executed locally. The exploit has been made available to the public and could be exploited. This patch is called 16357. It is best practice to apply a patch to resolve this issue.	2025-10-16	4.8
CVE-2025-10986	ivanti - multiple products	Path traversal in the admin panel of Ivanti EPMM before version 12.6.0.2, 12.5.0.4, and 12.4.0.4 allows a remote authenticated attacker with admin privileges to write data in unintended locations on disk.	2025-10-14	4.7
CVE-2025-31366	fortinet - multiple products	An Improper Neutralization of Input During Web Page Generation vulnerability [CWE-79] in FortiOS 7.6.0 through 7.6.3, 7.4.0 through 7.4.7, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiProxy 7.6.0 through 7.6.3, 7.4.0 through 7.4.9, 7.2 all versions, 7.0 all versions; FortiSASE 25.3.a may allow an unauthenticated attacker to perform a reflected cross site scripting (XSS) via crafted HTTP requests.	2025-10-14	4.7
CVE-2025-58719	microsoft - multiple products	Use after free in Connected Devices Platform Service (Cdpsvc) allows an authorized attacker to elevate privileges locally.	2025-10-14	4.7
CVE-2025-43280	apple - multiple products	The issue was resolved by not loading remote images This issue is fixed in iOS 18.6 and iPadOS 18.6. Forwarding an email could display remote images in Mail in Lockdown Mode.	2025-10-15	4.7
CVE-2025-60013	f5 - multiple products	When a user attempts to initialize the rSeries FIPS module using a password with special shell metacharacters, the FIPS hardware security module (HSM) may fail to initialize. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-10-15	4.6
CVE-2025-11568	red hat - multiple products	A data corruption vulnerability has been identified in the luksmeta utility when used with the LUKS1 disk encryption format. An attacker with the necessary permissions can exploit this flaw by writing a large amount of metadata to an encrypted device. The utility fails to correctly validate the available space, causing the metadata to overwrite and corrupt the user's encrypted data. This action leads to a permanent loss of the stored information. Devices using the LUKS formats other than LUKS1 are not affected by this issue.	2025-10-15	4.4
CVE-2025-46752	fortinet - fortidlp_agent	A insertion of sensitive information into log file in Fortinet FortiDLP 12.0.0 through 12.0.5, 11.5.1, 11.4.6, 11.4.5 allows attacker to information disclosure via re-using the enrollment code.	2025-10-16	4.4

CVE-2024-47569	fortinet - multiple products	A insertion of sensitive information into sent data in Fortinet FortiManager Cloud 7.4.1 through 7.4.3, FortiVoice 7.0.0 through 7.0.4, 6.4.0 through 6.4.9, 6.0.7 through 6.0.12, FortiMail 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.9, FortiOS 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.8, 7.0.0 through 7.0.15, 6.4.0 through 6.4.15, 6.2.0 through 6.2.17, 6.0.0 through 6.0.18, FortiWeb 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.11, 7.0.0 through 7.0.11, 6.4.0 through 6.4.3, FortiRecorder 7.2.0 through 7.2.1, 7.0.0 through 7.0.4, FortiNDR 7.6.0 through 7.6.1, 7.4.0 through 7.4.8, 7.2.0 through 7.2.5, 7.1.0 through 7.1.1, 7.0.0 through 7.0.7, 1.5.0 through 1.5.3, FortiPAM 1.3.0 through 1.3.1, 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiTester 7.4.0 through 7.4.2, 7.3.0 through 7.3.2, 7.2.0 through 7.2.3, 7.1.0 through 7.1.1, 7.0.0, 4.2.0 through 4.2.1, FortiProxy 7.4.0 through 7.4.4, 7.2.0 through 7.2.10, 7.0.0 through 7.0.21, 2.0.0 through 2.0.14, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7, FortiManager 7.6.0 through 7.6.1, 7.4.1 through 7.4.3 allows attacker to disclose sensitive information via specially crafted packets.	2025-10-14	4.3
CVE-2025-25255	fortinet - fortiproxy	An Improperly Implemented Security Check for Standard vulnerability [CWE-358] in FortiProxy 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0.1 through 7.0.21, and FortiOS 7.6.0 through 7.6.3 explicit web proxy may allow an authenticated proxy user to bypass the domain fronting protection feature via crafted HTTP requests.	2025-10-14	4.3
CVE-2025-54822	fortinet - multiple products	An improper authorization vulnerability [CWE-285] in Fortinet FortiOS version 7.4.0 through 7.4.1 and before 7.2.8 & Fortinet FortiProxy before version 7.4.8 allows an authenticated attacker to access static files of others VDOMs via crafted HTTP or HTTPS requests.	2025-10-14	4.3
CVE-2025-9640	red hat - multiple products	A flaw was found in Samba, in the vfs_streams_xattr module, where uninitialized heap memory could be written into alternate data streams. This allows an authenticated user to read residual memory content that may include sensitive data, resulting in an information disclosure vulnerability.	2025-10-15	4.3
CVE-2025-41254	vmware - Spring Framework	STOMP over WebSocket applications may be vulnerable to a security bypass that allows an attacker to send unauthorized messages. Affected Spring Products and VersionsSpring Framework: * 6.2.0 - 6.2.11 * 6.1.0 - 6.1.23 * 6.0.x - 6.0.29 * 5.3.0 - 5.3.45 * Older, unsupported versions are also affected. MitigationUsers of affected versions should upgrade to the corresponding fixed version. Affected version(s)Fix versionAvailability6.2.x6.2.12OSS6.1.x6.1.24 Commercial https://enterprise.spring.io/ 6.0.xN/A Out of support https://spring.io/projects/spring-framework#support 5.3.x5.3.46 Commercial https://enterprise.spring.io/ No further mitigation steps are necessary. CreditThis vulnerability was discovered and responsibly reported by Jannis Kaiser.	2025-10-16	4.3
CVE-2025-58132	zoom - multiple products	Command injection in some Zoom Clients for Windows may allow an authenticated user to conduct a disclosure of information via network access.	2025-10-15	4.1
CVE-2025-2138	ibm - multiple products	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user on the network to delete comments from other users due to client-side enforcement of server-side security.	2025-10-12	3.5
CVE-2025-2139	ibm - multiple products	IBM Engineering Requirements Management Doors Next 7.0.2, 7.0.3, and 7.1 could allow an authenticated user on the network to delete reviews from other users due to client-side enforcement of server-side security.	2025-10-12	3.5
CVE-2025-59284	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows NTLM allows an unauthorized attacker to perform spoofing locally.	2025-10-14	3.3
CVE-2025-59280	microsoft - multiple products	Improper authentication in Windows SMB Client allows an unauthorized attacker to perform tampering over a network.	2025-10-14	3.1
CVE-2025-54196	adobe - connect	Adobe Connect versions 12.9 and earlier are affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. An attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction in that a victim must click on a crafted link.	2025-10-14	3.1
CVE-2025-2529	ibm - Terracotta	Applications using affected versions of Ehcache 3.x can experience degraded cache-write performance if the application using Ehcache utilizes keys sourced from (malicious) external parties in an unfiltered/unsalted way.	2025-10-15	2.9
CVE-2025-31514	fortinet - fortios	An Insertion of Sensitive Information into Log File vulnerability [CWE-532] in FortiOS 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0 all versions, 6.4 all versions may allow an attacker with at least read-only privileges to retrieve sensitive 2FA-related information via observing logs or via diagnose command.	2025-10-14	2.7
CVE-2025-58903	fortinet - multiple products	An Unchecked Return Value vulnerability [CWE-252] in Fortinet FortiOS version 7.6.0 through 7.6.3 and before 7.4.8 API allows an authenticated user to cause a Null Pointer Dereference, crashing the http daemon via a specialy crafted request.	2025-10-14	2.7
CVE-2025-47890	fortinet - multiple products	An URL Redirection to Untrusted Site vulnerabilities [CWE-601] in FortiOS 7.6.0 through 7.6.2, 7.4.0 through 7.4.8, 7.2 all versions, 7.0 all versions, 6.4 all versions; FortiProxy 7.6.0 through 7.6.3, 7.4 all versions, 7.2 all versions, 7.0 all versions; FortiSASE 25.2.a may allow an unauthenticated attacker to perform an open redirect attack via crafted HTTP requests.	2025-10-14	2.6
CVE-2025-6026	lenovo - Universal Device Client	An improper certificate validation vulnerability was reported in the Lenovo Universal Device Client (UDC) that could allow a user capable of intercepting network traffic to obtain application metadata, including device information, geolocation, and telemetry data.	2025-10-15	2.3
CVE-2025-59294	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Taskbar Live allows an unauthorized attacker to disclose information with a physical attack.	2025-10-14	2.1

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.