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 14 سبتمبر إلى 20 سبتمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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 14th of September to 20th of September. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-31255	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in tvOS 26, macOS Sonoma 14.8, macOS Sequoia 15.7, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to access sensitive user data.	2025-09-15	9.8
CVE-2025-43342	apple - multiple products	A correctness issue was addressed with improved checks. This issue is fixed in tvOS 26, Safari 26, iOS 18.7 and iPadOS 18.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing maliciously crafted web content may lead to an unexpected process crash.	2025-09-15	9.8
CVE-2025-43343	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in tvOS 26, Safari 26, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing maliciously crafted web content may lead to an unexpected process crash.	2025-09-15	9.8
CVE-2025-43347	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in tvOS 26, watchOS 26, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An input validation issue was addressed.	2025-09-15	9.8
CVE-2025-43359	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in tvOS 26, macOS Sonoma 14.8, macOS Sequoia 15.7, iOS 18.7 and iPadOS 18.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. A UDP server socket bound to a local interface may become bound to all interfaces.	2025-09-15	9.8
CVE-2025-43362	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 18.7 and iPadOS 18.7, iOS 26 and iPadOS 26. An app may be able to monitor keystrokes without user permission.	2025-09-15	9.8
CVE-2025-9242	watchguard - Fireware OS	An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the Mobile User VPN with IKEv2 and the Branch Office VPN using IKEv2 when configured with a dynamic gateway peer.This vulnerability affects Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.3 and 2025.1.	2025-09-17	9.3
CVE-2025-43329	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 26, tvOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to break out of its sandbox.	2025-09-15	8.8
CVE-2025-43358	apple - multiple products	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, iOS 18.7 and iPadOS 18.7, macOS Tahoe 26, iOS 26 and iPadOS 26. A shortcut may be able to bypass sandbox restrictions.	2025-09-15	8.8
CVE-2025-10533	mozilla - multiple products	This vulnerability affects Firefox < 143, Firefox ESR < 115.28, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	8.8
CVE-2025-10537	mozilla - multiple products	Memory safety bugs present in Firefox ESR 140.2, Thunderbird ESR 140.2, Firefox 142 and Thunderbird 142. 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 < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	8.8
CVE-2025-37123	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the command-line interface of HPE Aruba Networking EdgeConnect SD-WAN Gateways could allow an authenticated remote attacker to escalate privileges. Successful exploitation of this vulnerability may enable the attacker to execute arbitrary system commands with root privileges on the underlying operating system.	2025-09-16	8.8
CVE-2025-37124	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the HPE Aruba Networking SD-WAN Gateways could allow an unauthenticated remote attacker to bypass firewall protections. Successful exploitation could allow an attacker to route potentially harmful traffic through the internal network, leading to unauthorized access or disruption of services.	2025-09-16	8.6

CVE-2025-43330	apple - macos	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7, macOS Tahoe 26. An app may be able to break out of its sandbox.	2025-09-15	8.2
CVE-2025-43371	apple - xcode	This issue was addressed with improved checks. This issue is fixed in Xcode 26. An app may be able to break out of its sandbox.	2025-09-15	8.2
CVE-2025-10534	mozilla - multiple products	This vulnerability affects Firefox < 143 and Thunderbird < 143.	2025-09-16	8.1
CVE-2025-43204	apple - macos	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Tahoe 26. An app may be able to break out of its sandbox.	2025-09-15	7.8
CVE-2025-43286	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to break out of its sandbox.	2025-09-15	7.8
CVE-2025-43298	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to gain root privileges.	2025-09-15	7.8
CVE-2025-43316	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26, visionOS 26. A malicious app may be able to gain root privileges.	2025-09-15	7.8
CVE-2025-43333	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to gain root privileges.	2025-09-15	7.8
CVE-2025-43340	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to break out of its sandbox.	2025-09-15	7.8
CVE-2025-43341	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to gain root privileges.	2025-09-15	7.8
CVE-2025-43372	apple - multiple products	The issue was addressed with improved input validation. This issue is fixed in tvOS 26, watchOS 26, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	2025-09-15	7.8
CVE-2025-54262	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.3 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.	2025-09-16	7.8
CVE-2025-24088	apple - macos	The issue was addressed by adding additional logic. This issue is fixed in macOS Tahoe 26. An app may be able to override MDM-enforced settings from profiles.	2025-09-15	7.5
CVE-2025-31271	apple - macos	This issue was addressed through improved state management. This issue is fixed in macOS Tahoe 26. Incoming FaceTime calls can appear or be accepted on a locked macOS device, even with notifications disabled on the lock screen.	2025-09-15	7.5
CVE-2025-41248	vmware - Spring Security	The Spring Security annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue when using @PreAuthorize and other method security annotations, resulting in an authorization bypass. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in generic superclasses or generic interfaces. This CVE is published in conjunction with CVE-2025-41249 https://spring.io/security/cve-2025-41249 .	2025-09-16	7.5
CVE-2025-41249	vmware - Spring Framework	The Spring Framework annotation detection mechanism may not correctly resolve annotations on methods within type hierarchies with a parameterized super type with unbounded generics. This can be an issue if such annotations are used for authorization decisions. Your application may be affected by this if you are using Spring Security's @EnableMethodSecurity feature. You are not affected by this if you are not using @EnableMethodSecurity or if you do not use security annotations on methods in generic superclasses or generic interfaces. This CVE is published in conjunction with CVE-2025-41248 https://spring.io/security/cve-2025-41248 .	2025-09-16	7.5
CVE-2025-10535	mozilla - firefox	This vulnerability affects Firefox < 143.	2025-09-16	7.5
CVE-2025-37125	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A broken access control vulnerability exists in HPE Aruba Networking EdgeConnect OS (ECOS). Successful exploitation could allow an attacker to bypass firewall protections, potentially leading to unauthorized traffic being handled improperly	2025-09-16	7.5
CVE-2025-26515	netapp - multiple products	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 without Single Sign-on enabled are susceptible to a Server-Side Request Forgery (SSRF) vulnerability. Successful exploit could allow an unauthenticated attacker to change the password of any Grid Manager or Tenant Manager non-federated user.	2025-09-19	7.5
CVE-2025-36244	ibm - multiple products	IBM AIX 7.2, 7.3, IBM VIOS 3.1, and 4.1, when configured to use Kerberos network authentication, could allow a local user to write to files on the system with root privileges due to improper initialization of critical variables.	2025-09-16	7.4
CVE-2025-4953	red hat - multiple products	A flaw was found in Podman. In a Containerfile or Podman, data written to RUN --mount=type=bind mounts during the podman build is not discarded. This issue can lead to files created within the container appearing in the temporary build context directory on the host, leaving the created files accessible.	2025-09-16	7.4

CVE-2025-10528	mozilla - multiple products	This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	7.3
CVE-2025-37126	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability exists in the HPE Aruba Networking EdgeConnect SD-WAN Gateways Command Line Interface that allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of this vulnerability will result in the ability to execute arbitrary commands as root on the underlying operating system.	2025-09-16	7.2
CVE-2025-37127	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the cryptographic logic used by HPE Aruba Networking EdgeConnect SD-WAN Gateways could allow an authenticated remote attacker to gain shell access. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system, potentially leading to unauthorized access and control over the affected systems.	2025-09-16	7.2
CVE-2025-43263	apple - xcode	The issue was addressed with improved checks. This issue is fixed in Xcode 26. An app may be able to read and write files outside of its sandbox.	2025-09-15	7.1
CVE-2025-43287	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26. Processing a maliciously crafted image may corrupt process memory.	2025-09-15	7.1
CVE-2025-10527	mozilla - multiple products	This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	7.1
CVE-2025-43304	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to gain root privileges.	2025-09-15	7.0
CVE-2025-59215	microsoft - multiple products	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-18	7.0
CVE-2025-59216	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2025-09-18	7.0
CVE-2025-59220	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2025-09-18	7.0
CVE-2025-43793	liferay - multiple products	Liferay Portal 7.4.0 through 7.4.3.105, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions may incorrectly identify the subdomain of a domain name and create a supercookie, which allows remote attackers who control a website that share the same TLD to read cookies set by the application.	2025-09-15	6.9
CVE-2025-43799	liferay - multiple products	Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92 and 7.3 GA through update 35, and older unsupported versions does not limit access to APIs before a user has changed their initial password, which allows remote users to access and edit content via the API.	2025-09-15	6.9
CVE-2025-6999	watchguard - Fireware OS	An HTTP Request Smuggling [CWE-444] vulnerability in the Authentication portal of WatchGuard Fireware OS allows a remote attacker to evade request parameter sanitation and perform a reflected self-Cross-Site Scripting (XSS) attack.This issue affects Fireware OS: from 12.0 through 12.11.2.	2025-09-15	6.9
CVE-2025-43801	liferay - multiple products	Unchecked input for loop condition vulnerability in XML-RPC in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions allows remote attackers to perform a denial-of-service (DoS) attacks via a crafted XML-RPC request.	2025-09-16	6.9
CVE-2025-43805	liferay - multiple products	Liferay Portal 7.3.0 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, and 7.3 GA through update 35 does not perform an authorization check when users attempt to view a display page template, which allows remote attackers to view display page templates via crafted URLs.	2025-09-16	6.9
CVE-2025-43803	liferay - multiple products	Insecure direct object reference (IDOR) vulnerability in the Contacts Center widget in Liferay Portal 7.4.0 through 7.4.3.119, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.6, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and older unsupported versions allows remote attackers to view contact information, including the contact's name and email address, via the _com_liferay_contacts_web_portlet_ContactsCenterPortlet_entryId parameter.	2025-09-19	6.9
CVE-2025-43808	liferay - multiple products	The Commerce component in Liferay Portal 7.3.0 through 7.4.3.112, and Liferay DXP 2023.Q4.0 through 2023.Q4.8, 2023.Q3.1 through 2023.Q3.10, 7.4 GA through update 92, and 7.3 service pack 3 through update 35 saves virtual products uploaded to Documents and Media with guest view permission, which allows remote attackers to access and download virtual products for free via a crafted URL.	2025-09-19	6.9
CVE-2025-37128	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the web API of HPE Aruba Networking EdgeConnect SD-WAN Gateways could allow an authenticated remote attacker to terminate arbitrary running processes. Successful exploitation could allow an attacker to disrupt system operations, potentially resulting in an unstable system state.	2025-09-16	6.8
CVE-2025-36035	ibm - PowerVM Hypervisor	IBM PowerVM Hypervisor FW950.00 through FW950.E0, FW1050.00 through FW1050.50, and FW1060.00 through FW1060.40 could allow a local privileged user to cause a denial of service by issuing a specially crafted IBM i hypervisor call that would disclose memory contents or consume excessive memory resources.	2025-09-14	6.7
CVE-2025-37129	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerable feature in the command line interface of EdgeConnect SD-WAN could allow an authenticated attacker to exploit built-in script execution capabilities. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system if the feature is enabled without proper security measures.	2025-09-16	6.7
CVE-2025-59328	apache - fory	A vulnerability in Apache Fory allows a remote attacker to cause a Denial of Service (DoS). The issue stems from the insecure deserialization of untrusted data. An attacker can supply a large, specially crafted data payload that, when processed, consumes an excessive amount of CPU resources during	2025-09-15	6.5

		the deserialization process. This leads to CPU exhaustion, rendering the application or system using the Apache Fory library unresponsive and unavailable to legitimate users. Users of Apache Fory are strongly advised to upgrade to version 0.12.2 or later to mitigate this vulnerability. Developers of libraries and applications that depend on Apache Fory should update their dependency requirements to Apache Fory 0.12.2 or later and release new versions of their software.		
CVE-2025-30468	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 26 and iPadOS 26. Private Browsing tabs may be accessed without authentication.	2025-09-15	6.5
CVE-2025-43272	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-09-15	6.5
CVE-2025-43327	apple - multiple products	The issue was addressed by adding additional logic. This issue is fixed in Safari 26, macOS Tahoe 26. Visiting a malicious website may lead to address bar spoofing.	2025-09-15	6.5
CVE-2025-43356	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in tvOS 26, Safari 26, iOS 18.7 and iPadOS 18.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. A website may be able to access sensor information without user consent.	2025-09-15	6.5
CVE-2025-10290	mozilla - firefox_focus	Opening links via the contextual menu in Focus iOS for certain URL schemes would fail to load but would not refresh the toolbar correctly, allowing attackers to spoof websites if users were coerced into opening a link explicitly through a long-press This vulnerability affects Focus for iOS < 143.0.	2025-09-16	6.5
CVE-2025-10529	mozilla - multiple products	This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	6.5
CVE-2025-10530	mozilla - multiple products	This vulnerability affects Firefox < 143 and Thunderbird < 143.	2025-09-16	6.5
CVE-2025-10532	mozilla - multiple products	This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	6.5
CVE-2025-37130	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in the command-line interface of EdgeConnect SD-WAN could allow an authenticated attacker to read arbitrary files within the system. Successful exploitation could allow an attacker to read sensitive data from the underlying file system.	2025-09-16	6.5
CVE-2025-26514	netapp - multiple products	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a Reflected Cross-Site Scripting vulnerability. Successful exploit could allow an attacker to view or modify configuration settings or add or modify user accounts but requires the attacker to know specific information about the target instance and then trick a privileged user into clicking a specially crafted link.	2025-09-19	6.4
CVE-2025-43279	apple - macos	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Tahoe 26. An app may be able to access user-sensitive data.	2025-09-15	6.2
CVE-2025-43297	apple - macos	A type confusion issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26. An app may be able to cause a denial-of-service.	2025-09-15	6.2
CVE-2025-43318	apple - macos	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Tahoe 26. An app with root privileges may be able to access private information.	2025-09-15	6.2
CVE-2025-10536	mozilla - multiple products	This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.	2025-09-16	6.2
CVE-2025-37122	hewlett packard enterprise (hpe) - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the web-based management interface of network access control services could allow an unauthenticated remote attacker to conduct a Reflected Cross-Site Scripting (XSS) attack. Successful exploitation could allow an attacker to execute arbitrary JavaScript code in a victim's browser in the context of the affected interface.	2025-09-17	6.1
CVE-2025-30755	oracle - opengrok	OpenGrok 1.14.1 has a reflected Cross-Site Scripting (XSS) issue when producing the cross reference page. This happens through improper handling of the revision parameter. The application reflects unsanitized user input into the HTML output.	2025-09-19	6.1
CVE-2025-59378	gnu - Guix	In guix-daemon in GNU Guix before 1618ca7, a content-addressed-mirrors file can be written to create a setuid program that allows a regular user to gain the privileges of the build user that runs it (even after the build has ended).	2025-09-15	5.7
CVE-2025-24197	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-31268	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-31269	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-31270	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-43190	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sonoma 14.8, macOS Sequoia 15.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43207	apple - macos	This issue was addressed with improved entitlements. This issue is fixed in macOS Tahoe 26. An app may be able to access user-sensitive data.	2025-09-15	5.5
CVE-2025-43208	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to read sensitive location information.	2025-09-15	5.5
CVE-2025-43231	apple - macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.8. An app may be able to access user-sensitive data.	2025-09-15	5.5
CVE-2025-43285	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5

CVE-2025-43291	apple - multiple products	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to modify protected parts of the file system.	2025-09-15	5.5
CVE-2025-43292	apple - macos	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7, macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43293	apple - multiple products	The issue was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43295	apple - multiple products	A denial-of-service issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26, iOS 18.7 and iPadOS 18.7. An app may be able to cause a denial-of-service.	2025-09-15	5.5
CVE-2025-43299	apple - multiple products	A denial-of-service issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26, iOS 18.7 and iPadOS 18.7. An app may be able to cause a denial-of-service.	2025-09-15	5.5
CVE-2025-43302	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 26, macOS Sonoma 14.8, macOS Sequoia 15.7, iOS 18.7 and iPadOS 18.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to cause unexpected system termination.	2025-09-15	5.5
CVE-2025-43303	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in tvOS 26, watchOS 26, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43305	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. A malicious app may be able to access private information.	2025-09-15	5.5
CVE-2025-43312	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to cause unexpected system termination.	2025-09-15	5.5
CVE-2025-43314	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43315	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access user-sensitive data.	2025-09-15	5.5
CVE-2025-43317	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in tvOS 26, watchOS 26, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43319	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-43321	apple - multiple products	The issue was resolved by blocking unsigned services from launching on Intel Macs. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-43325	apple - macos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43326	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43337	apple - macos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43346	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in tvOS 26, watchOS 26, iOS 18.7 and iPadOS 18.7, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	2025-09-15	5.5
CVE-2025-43353	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. Processing a maliciously crafted string may lead to heap corruption.	2025-09-15	5.5
CVE-2025-43354	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in tvOS 26, watchOS 26, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to access sensitive user data.	2025-09-15	5.5
CVE-2025-43355	apple - multiple products	A type confusion issue was addressed with improved memory handling. This issue is fixed in tvOS 26, macOS Sonoma 14.8, macOS Sequoia 15.7, iOS 18.7 and iPadOS 18.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to cause a denial-of-service.	2025-09-15	5.5
CVE-2025-43366	apple - macos	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Tahoe 26. An app may be able to disclose coprocessor memory.	2025-09-15	5.5
CVE-2025-43367	apple - multiple products	A privacy issue was addressed by moving sensitive data. This issue is fixed in macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-43369	apple - macos	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.5
CVE-2025-43375	apple - xcode	The issue was addressed with improved checks. This issue is fixed in Xcode 26. Processing an overly large path value may crash a process.	2025-09-15	5.5
CVE-2025-54237	adobe - substance_3d_stager	Substance3D - Stager versions 3.1.3 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. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2025-09-16	5.5
CVE-2025-36139	ibm - watsonx.data	IBM Lakehouse (watsonx.data 2.2) is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-18	5.5
CVE-2025-31254	apple - multiple products	This issue was addressed with improved URL validation. This issue is fixed in Safari 26, iOS 26 and iPadOS 26. Processing maliciously crafted web content may lead to unexpected URL redirection.	2025-09-15	5.4
CVE-2025-10531	mozilla - multiple products	This vulnerability affects Firefox < 143 and Thunderbird < 143.	2025-09-16	5.4

CVE-2025-36248	ibm - Copy Services Manager	IBM Copy Services Manager 6.3.13 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-09-19	5.4
CVE-2025-26517	netapp - multiple products	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a privilege escalation vulnerability. Successful exploit could allow an unauthorized authenticated attacker to discover Grid node names and IP addresses or modify Storage Grades.	2025-09-19	5.4
CVE-2025-10440	d-link - multiple products	A vulnerability has been found in D-Link DI-8100, DI-8100G, DI-8200, DI-8200G, DI-8003 and DI-8003G 16.07.26A1/17.12.20A1/19.12.10A1. Affected by this vulnerability is the function sub_4621DC of the file usb_paswd.asp of the component jhttpd. The manipulation of the argument hname leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-09-15	5.3
CVE-2025-10441	d-link - multiple products	A vulnerability was found in D-Link DI-8100G, DI-8200G and DI-8003G 17.12.20A1/19.12.10A1. Affected by this issue is the function sub_433F7C of the file version_upgrade.asp of the component jhttpd. The manipulation of the argument path results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used.	2025-09-15	5.3
CVE-2025-43797	liferay - multiple products	In Liferay Portal 7.1.0 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions, the default membership type of a newly created site is “Open” which allows any registered users to become a member of the site. A remote attacker with site membership can potentially view, add or edit content on the site.	2025-09-15	5.3
CVE-2025-43308	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	5.3
CVE-2025-10689	d-link - DIR-645	A vulnerability was identified in D-Link DIR-645 105B01. This issue affects the function soapcgi_main of the file /soap.cgi. Such manipulation of the argument service leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-09-18	5.3
CVE-2025-26516	netapp - multiple products	StorageGRID (formerly StorageGRID Webscale) versions prior to 11.8.0.15 and 11.9.0.8 are susceptible to a Denial of Service vulnerability. Successful exploit could allow an unauthenticated attacker to cause a Denial of Service on the Admin node.	2025-09-19	5.3
CVE-2025-43332	apple - multiple products	A file quarantine bypass was addressed with additional checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to break out of its sandbox.	2025-09-15	5.2
CVE-2025-43262	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26. USB Restricted Mode may not be applied to accessories connected during boot.	2025-09-15	5.1
CVE-2025-43311	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	5.1
CVE-2025-43804	liferay - multiple products	Cross-site scripting (XSS) vulnerability in Search widget in Liferay Portal 7.4.3.93 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_portal_search_web_portlet_SearchPortlet_userId parameter.	2025-09-16	5.1
CVE-2025-43809	liferay - multiple products	Cross-Site Request Forgery (CSRF) vulnerability in the server (license) registration page in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0 through 2023.Q4.7, 2023.Q3.1 through 2023.Q3.9, 7.4 GA through update 92, and older unsupported versions allows remote attackers to register a server license via the 'orderUuid' parameter.	2025-09-19	5.1
CVE-2025-37131	hewlett packard enterprise (hpe) - HPE Aruba Networking EdgeConnect SD-WAN Gateway	A vulnerability in EdgeConnect SD-WAN ECOS could allow an authenticated remote threat actor with admin privileges to access sensitive unauthorized system files. Under certain conditions, this could lead to exposure and exfiltration of sensitive information.	2025-09-16	4.9
CVE-2025-43791	liferay - multiple products	Multiple cross-site scripting (XSS) vulnerabilities in Liferay Portal 7.3.0 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92 and 7.3 GA through update 36 allow remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a "Rich Text" type field to (1) a web content structure, (2) a Documents and Media Document Type , or (3) custom assets that uses the Data Engine's module Rich Text field.	2025-09-15	4.8
CVE-2025-43800	liferay - multiple products	Cross-site scripting (XSS) vulnerability in Objects in Liferay Portal 7.4.3.20 through 7.4.3.111, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4 and 7.4 GA through update 92 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an object with a rich text type field.	2025-09-15	4.8
CVE-2025-43802	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in a custom object’s /o/c/<object-name> API endpoint in Liferay Portal 7.4.3.51 through 7.4.3.109, and Liferay DXP 2023.Q3.1 through 2023.Q3.4, 7.4 update 51 through update 92, and 7.3 update 33 through update 35. allows remote attackers to inject arbitrary web script or HTML via the externalReferenceCode parameter.	2025-09-15	4.8
CVE-2025-6947	watchguard - Fireware OS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WatchGuard Fireware OS allows Stored XSS via the SIP Proxy module. This vulnerability requires an authenticated administrator session to a locally managed Firebox. This issue affects Firebox: from 12.0 through 12.11.2.	2025-09-15	4.8
CVE-2025-47967	microsoft - Microsoft Edge (Chromium-based)	Insufficient ui warning of dangerous operations in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	2025-09-16	4.7
CVE-2025-36143	ibm - watsonx.data	IBM Lakehouse (watsonx.data 2.2) could allow an authenticated privileged user to execute arbitrary commands on the system due to improper validation of user supplied input.	2025-09-18	4.7
CVE-2025-43794	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in Liferay Portal 7.4.0 through 7.4.3.111, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through	2025-09-15	4.6

		update 92, 7.3 GA through update 35, and older unsupported versions allows remote authenticated attackers with the instance administrator role to inject arbitrary web script or HTML into all pages via a crafted payload injected into the Instance Configuration's (1) CDN Host HTTP text field or (2) CDN Host HTTPS text field.		
CVE-2025-43310	apple - multiple products	A configuration issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to trick a user into copying sensitive data to the pasteboard.	2025-09-15	4.4
CVE-2025-43368	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2025-09-15	4.3
CVE-2025-36146	ibm - watsonx.data	IBM Lakehouse (watsonx.data 2.2) could allow an authenticated user to obtain sensitive server component version information which could aid in further attacks against the system.	2025-09-18	4.3
CVE-2025-10630	grafana - grafana-zabbix-plugin	Grafana is an open-source platform for monitoring and observability. Grafana-Zabbix is a plugin for Grafana allowing to visualize monitoring data from Zabbix and create dashboards for analyzing metrics and realtime monitoring. Versions 5.2.1 and below contained a ReDoS vulnerability via user-supplied regex query which could causes CPU usage to max out. This vulnerability is fixed in version 6.0.0.	2025-09-19	4.3
CVE-2025-36082	ibm - multiple products	IBM OpenPages 9.0 and 9.1 allows web page cache to be stored locally which can be read by another user on the system.	2025-09-15	4.0
CVE-2025-24133	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 26 and iPadOS 26. Keyboard suggestions may display sensitive information on the lock screen.	2025-09-15	4.0
CVE-2025-43203	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in iOS 18.7 and iPadOS 18.7, iOS 26 and iPadOS 26. An attacker with physical access to an unlocked device may be able to view an image in the most recently viewed locked note.	2025-09-15	4.0
CVE-2025-43307	apple - macos	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	4.0
CVE-2025-43331	apple - macos	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to access protected user data.	2025-09-15	4.0
CVE-2025-43370	apple - xcode	A path handling issue was addressed with improved validation. This issue is fixed in Xcode 26. Processing an overly large path value may crash a process.	2025-09-15	4.0
CVE-2025-49728	microsoft - Microsoft PC Manager	Cleartext storage of sensitive information in Microsoft PC Manager allows an unauthorized attacker to bypass a security feature locally.	2025-09-16	4.0
CVE-2025-43283	apple - macos	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Tahoe 26. An app may be able to cause unexpected system termination.	2025-09-15	3.3
CVE-2025-43294	apple - macos	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	3.3
CVE-2025-43301	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.7, macOS Sonoma 14.8, macOS Tahoe 26. An app may be able to access contact info related to notifications in Notification Center.	2025-09-15	3.3
CVE-2025-43328	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26. An app may be able to access sensitive user data.	2025-09-15	3.3
CVE-2025-43344	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in tvOS 26, watchOS 26, visionOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to cause unexpected system termination.	2025-09-15	3.3
CVE-2025-43357	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Tahoe 26, iOS 26 and iPadOS 26. An app may be able to fingerprint the user.	2025-09-15	3.3
CVE-2025-43349	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in tvOS 26, macOS Sonoma 14.8, macOS Sequoia 15.7, iOS 18.7 and iPadOS 18.7, visionOS 26, watchOS 26, macOS Tahoe 26, iOS 26 and iPadOS 26. Processing a maliciously crafted video file may lead to unexpected app termination.	2025-09-15	2.8
CVE-2025-0164	ibm - multiple products	IBM QRadar SIEM 7.5 through 7.5 Update Pack 13 Independent Fix 01 could allow a local privileged user to perform unauthorized actions on configuration files due to improper permission assignment.	2025-09-14	2.3
CVE-2025-43792	liferay - multiple products	Remote staging in Liferay Portal 7.4.0 through 7.4.3.105, and older unsupported versions, and Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92, 7.3 GA through update 35, and older unsupported versions does not properly obtain the remote address of the live site from the database which, which allows remote authenticated users to exfiltrate data to an attacker controlled server (i.e., a fake “live site”) via the _com_liferay_exportimport_web_portlet_ExportImportPortlet_remoteAddress and _com_liferay_exportimport_web_portlet_ExportImportPortlet_remotePort parameters. To successfully exploit this vulnerability, an attacker must also successfully obtain the staging server’s shared secret and add the attacker controlled server to the staging server’s whitelist.	2025-09-15	2.3
CVE-2025-43798	liferay - DXP	Liferay DXP 2023.Q4.0, 2023.Q3.1 through 2023.Q3.4, 7.4 GA through update 92 and 7.3 GA through update 35 allows a time-based one-time password (TOTP) to be used multiple times during the validity period, which allows attackers with access to a user’s TOTP to authenticate as the user.	2025-09-15	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.